S03P(006W000

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平11－31130

(43)公開日　平成11年(1999)２月２日

(51)Int.Cl.⁶	識別記号	ＦＩ	
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｂ
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｂ
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｂ

審査請求　未請求　請求項の数21　ＯＬ　（全 44 頁）

(21)出願番号　特願平9－184866

(22)出願日　平成９年(1997)７月10日

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号

(72)発明者　河野　健二
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内

(72)発明者　中垣　寿平
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内

(72)発明者　小島　俊一
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内

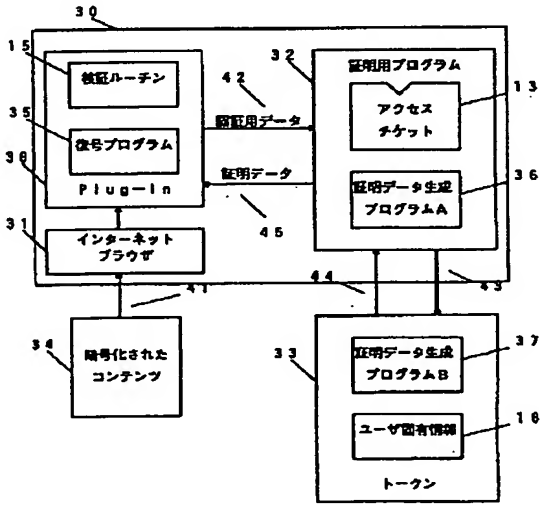
(74)代理人　弁理士　澤田　俊夫

(54)【発明の名称】　サービス提供装置

(57)【要約】

【課題】　ユーザおよびサービス提供者の負担を最小限に押さえながら、サービスの利用を正当な権利を有するユーザにのみ提供する。

【解決手段】　インターネットブラウザ３１のプラグイン３８が起動すると、プラグイン３８中の検証プログラム１５が起動し、証明用プログラム３２と通信してユーザ認証を行う。証明用プログラム３２の証明データ生成プログラムＡ３６は、トークン３３中の証明データ生成プログラムＢ３７と協調して、ユーザ固有情報１６とアクセスチケット１３とに基づいて計算を行い、その計算に基づいてプラグイン３８中の検証プログラム１５と通信を行う。通信の結果、検証プログラム１５による認証が成功するのは、ユーザ固有情報と、アクセスチケットと、暗号化されたコンテンツとの３つが正しく対応している場合に限られる。



1

【特許請求の範囲】

【請求項１】　正当な権利を有するユーザのみにサービスを提供するサービス提供装置において、
認証用データを記憶する第１の記憶手段と、
ユーザの固有情報を記憶する第２の記憶手段と、
前記ユーザの固有情報と、アクセス資格認証の特徴情報とに対し、所定の計算を実行した実行結果である証明用補助情報を記憶する第３の記憶手段と、
前記第１の記憶手段に保持されている認証用データと、前記第２の記憶手段に記憶されている前記ユーザの固有情報と、前記第３の記憶手段に記憶されている前記証明用補助情報とに所定の計算を施して証明データを生成する証明データ生成手段とを有し、
前記証明データ生成手段によって生成された証明データを利用してサービスを提供することを特徴とするサービス提供装置。

【請求項２】　正当な権利を有するユーザのみにサービスを提供するサービス提供装置において、
認証用データを記憶する第１の記憶手段と、
ユーザの固有情報を記憶する第２の記憶手段と、
前記ユーザの固有情報と、アクセス資格認証の特徴情報とに対し、所定の計算を実行した実行結果である証明用補助情報を記憶する第３の記憶手段と、
前記第１の記憶手段に保持されている認証用データと、前記第２の記憶手段に記憶されている前記ユーザの固有情報と、前記第３の記憶手段に記憶されている前記証明用補助情報とに所定の計算を施して証明データを生成する証明データ生成手段と、
前記証明データ生成手段によって生成された証明データが前記アクセス資格認証の特徴情報に基づいて生成されていることを検証する証明データ検証手段とを有し、
前記証明データ検証手段による検証が成功した場合にのみ、サービスを提供することを特徴とするサービス提供装置。

【請求項３】　利用を制限された情報を入力する入力手段を更に有し、
前記証明データ検証手段による検証が成功した場合にのみ、前記情報に対する利用の制限を解除して情報の利用を可能にすることを特徴とする請求項２に記載のサービス提供装置。

【請求項４】　前記アクセス資格認証の特徴情報が暗号化関数における復号鍵であり、前記認証用データが適当なデータを前記復号鍵に対応する暗号化鍵を用いて暗号化したものであり、
前記証明データ検証手段は、前記証明データ生成手段が生成する証明データが前記認証用データを正しく復号したものである場合に検証が成功したと判定することを特徴とする請求項２または３に記載のサービス提供装置。

【請求項５】　前記アクセス資格認証の特徴情報が暗号化関数における暗号化鍵であり、

2

前記証明データ検証手段は、前記証明データ生成手段が生成する証明データが前記認証用データを正しく暗号化したものである場合に検証が成功したと判定することを特徴とする請求項２または３に記載のサービス提供装置。

【請求項６】　前記アクセス資格認証の特徴情報は、デジタル署名関数における署名鍵であり、前記証明データ検証手段は、前記証明データ生成手段が生成する証明データが、前記認証用データに対して、前記署名鍵を用いて正しく生成されたデジタル署名であることが検証された場合に検証が成功したと判定することを特徴とする請求項２または３に記載のサービス提供装置。

【請求項７】　前記利用を制限された情報は、少なくとも一部が暗号化された情報であり、
前記証明データ検証手段による検証が成功した場合にのみ、前記暗号化された情報を復号して情報の利用を可能にすることを特徴とする請求項２乃至６に記載のサービス提供装置。

【請求項８】　暗号化された情報を入力する入力手段を更に有し、
前記アクセス資格認証の特徴情報が暗号化関数における第１の復号鍵であり、前記認証用データが前記暗号化された情報を復号する第２の復号鍵を前記第１の復号鍵に対応する暗号化鍵を用いて暗号化したものであり、
前記証明データ生成手段によって生成された証明データが前記第２の復号鍵であり、前記第２の復号鍵を用いて前記暗号化された情報を復号して、前記情報に対応するサービスを提供することを特徴とする請求項１または２に記載のサービス提供装置。

【請求項９】　前記暗号化関数が非対称鍵暗号化関数であり、前記アクセス資格認証の特徴情報が鍵の一方であることを特徴とする請求項４、５または８に記載のサービス提供装置。

【請求項１０】　前記暗号化関数が公開鍵暗号化関数であり、前記アクセス資格認証の特徴情報が秘密鍵であることを特徴とする請求項４、５または８に記載のサービス提供装置。

【請求項１１】　前記暗号化関数が対称鍵暗号化関数であり、前記アクセス資格認証の特徴情報が共通秘密鍵であることを特徴とする請求項４、５または８に記載のサービス提供装置。

【請求項１２】　証明データ生成装置および証明データ検証装置を具備し、前記証明データ生成装置および前記証明データ検証装置が通信を行ってユーザのアクセス資格を認証するアクセス資格認証装置を有するサービス提供装置において、
前記証明データ生成装置は、
認証用データを記憶する第１の記憶手段と、
ユーザの固有情報を記憶する第２の記憶手段と、
前記ユーザの固有情報と、アクセス資格認証の特徴情報

とに対して、所定の計算を実行した実行結果である証明用補助情報を記憶する第３の記憶手段と、
前記第１の記憶手段に保持されている前記認証用データと、前記第２の記憶手段に保持されている前記ユーザの固有情報と、前記第３の記憶手段に保持されている前記証明用補助情報とに所定の計算を実行して証明情報を生成する証明データ生成手段とを有し、
前記証明データ検証装置は、
認証用データを記憶する第４の記憶手段と、
証明データを記憶する第５の記憶手段と、
前記証明データ生成手段によって生成された前記証明データが前記アクセス資格認証用の特徴情報に基づいて生成されていることを検証する証明データ検証手段とを有し、
前記証明データ検証装置は、前記第４の記憶手段に記憶されている前記認証用データを前記証明データ生成装置の前記第１の記憶手段に書き出し、
前記証明データ生成装置は、前記証明データ生成手段によって前記第１の記憶手段に書き込まれた前記認証用データをもとに生成した前記証明データを、前記証明データ検証装置の前記第５の記憶手段に書き出し、
前記証明データ検証装置は前記第５の記憶手段に書き込まれた前記証明データを用いてユーザのアクセス資格を認証することを特徴とするサービス提供装置。
【請求項１３】　前記アクセス資格認証用の特徴情報が暗号化関数の復号鍵であり、
前記証明データ検証装置が乱数生成手段と、生成した乱数を記憶する第６の記憶手段と、認証用素データを記憶する第７の記憶手段とを備え、
前記乱数生成手段は生成した乱数を前記第６の記憶手段に書き込むと共に、前記第７の記憶手段に記憶されている前記認証用素データに前記乱数を用いた乱数効果を施した後、前記認証用データとして前記第４の記憶手段に書き込み、
前記証明データ検証手段は、前記第６の記憶手段に記憶されている前記乱数による乱数効果を、前記証明データ生成装置によって前記第５の記憶手段に書き込まれた前記証明データから除去した結果が、前記アクセス資格認証の特徴情報である復号鍵で前記第７の記憶手段に記憶されている前記認証用素データを復号したものであることを検証することを特徴とする請求項１２に記載のサービス提供装置。
【請求項１４】　前記アクセス資格認証用の特徴情報が暗号化関数の暗号化鍵であり、
前記証明データ検証装置が乱数生成手段を備え、前記乱数生成手段は生成した乱数を前記認証用データとして前記第４の記憶手段に書き込み、
前記証明データ検証手段は、前記証明データ生成装置によって前記第５の記憶手段に書き込まれた前記証明データが、前記乱数を復号したものであることを検証することを特徴とする請求項１２に記載のサービス提供装置。
【請求項１５】　前記アクセス資格認証用の特徴情報がデジタル署名関数の署名鍵であり、
前記証明データ検証装置が乱数生成手段を備え、前記乱数生成手段は生成した乱数を認証用データとして前記第４の記憶手段に書き込み、
前記証明データ検証手段は、前記証明データ生成装置によって前記第５の記憶手段に書き込まれた前記証明データが、前記乱数である認証用データに対する、前記アクセス資格認証の特徴情報である署名鍵によるデジタル署名であることを検証することを特徴とする請求項１２に記載のサービス提供装置。
【請求項１６】　少なくとも、前記第２の記憶手段と、前記証明データ生成手段とが、内部データおよび処理手続きを外部から観測することを困難ならしめる防御手段中に保存されていることを特徴とする請求項１乃至１５に記載のサービス提供装置。
【請求項１７】　少なくとも、前記第２の記憶手段と、前記証明データ生成手段とが、ＩＣカードなどの携帯可能な小型演算装置として構成されていることを特徴とする請求項１乃至１５に記載のサービス提供装置。
【請求項１８】　少なくとも、前記証明データ検証手段が、内部データおよび処理手続きを外部から観測することを困難ならしめる防御手段中に保存されていることを特徴とする請求項１乃至１５に記載のサービス提供装置。
【請求項１９】　少なくとも、前記証明データ検証手段が、ＩＣカードなどの携帯可能な小型演算装置として構成されていることを特徴とする請求項１乃至１５に記載のサービス提供装置。
【請求項２０】　前記入力手段から入力される情報は、イメージ、動画、音声、音楽などのマルチメディア情報または前記マルチメディアを暗号化したものであり、
前記サービスは、前記入力された情報を再生することを特徴とする請求項１乃至１９に記載のサービス提供装置。
【請求項２１】　前記証明データの生成を制御する利用制御情報を記憶する第８の記憶手段をさらに有し、
前記第３の記憶手段に保持されている前記証明用補助情報は、前記ユーザの固有情報と、前記アクセス資格認証の特徴情報と、前記利用制御情報とに対し、所定の計算を実行した実行結果であり、
前記証明データ生成手段は、前記第１の記憶手段に保持されている認証用データと、前記第２の記憶手段に記憶されている前記ユーザの固有情報と、前記第３の記憶手段に記憶されている前記証明用補助情報と、前記第８の記憶手段に記憶されている前記利用制御情報とに所定の計算を施して証明データを生成することを特徴とする請求項１乃至２０に記載のサービス提供装置。
【発明の詳細な説明】

【０００１】
【発明の属する技術分野】本発明は、正当な権利を有するユーザにのみ選択的にサービスを提供することのできるサービス提供装置およびその方法に関する。
【０００２】
【従来技術】近年のネットワークの発達によって、さまざまな情報がディジタル化されネットワークを通じて流通する時代が到来している。ディジタル化される情報としては、文字情報をはじめ静止画、動画、音声、プログラムなどがあり、我々はネットワーク上でこれらを組み合わせたさまざまなサービスを受けることが可能である。しかし、これらディジタル情報の大きな特徴であるコピーの容易性が、これまでネットワークでのディジタル情報の流通を阻害する要因となっていた。これは、ディジタル情報をコピーするとオリジナルとまったく同じ物を生成することができるため、一旦流通したものが著作者の意図しないところで無断で使用され、著作者が得るべき正当な対価を回収し難いという問題に起因する。
【０００３】この問題を解決するため、最近では日本アイ・ビー・エム（株）のＣＤ－ＳＨＯＷＣＡＳＥ（商標または製品名）のように、ディジタル情報を暗号化して自由に流通させ、利用する際には代金を支払って電話回線等で復号鍵を受け取り、ディジタル情報を利用するようなシステムも登場している。また、特公平６－９５３０２号公報の「ソフトウエア管理方式」には、ソフトウエアを利用した量に応じて課金し料金を回収するシステムの例が示されている。特公平７－２１２７６号公報の「情報利用量測定装置」では、放送によって配布された情報のすべての利用者の情報利用時間等の利用量を的確に測定することができる情報利用量測定装置について述べられている。これによると情報利用量測定装置は、暗号化された書籍情報を受信し蓄積し、ユーザが書籍情報を復号し表示した時間と量を利用履歴として記録しておきそれにより料金を徴収する例が示されている。
【０００４】前記のシステムを実現する方法として、さまざまな暗号技術やプログラムの実行制御技術が先行技術として知られている。
【０００５】プログラム実行制御技術は、
①アプリケーションプログラム中に、ユーザのアクセス資格認証のためのルーチンを埋め込み、
②該ルーチンはアプリケーションの実行を試みているユーザが正規の認証用の鍵を保有していることを検査し、
③前記認証用の鍵の存在が確認された場合に限りプログラムを続行し、それ以外の場合はプログラムの実行を停止する
技術である。当技術を利用することにより、認証鍵を保有する正規のユーザのみアプリケーションの実行を可能ならしめることができる。当技術は、ソフトウエア領布事業において実用化されており、製品としては、例えばＲａｉｎｂｏｗＴｅｃｈｎｏｌｏｇｉｅｓ，　Ｉｎｃ．社のＳｅｎｔｉｎｅｌ　ＳｕｐｅｒＰｒｏ（商標）や、Ａｌａｄｄｉｎ　Ｋｎｏｗｌｅｄｇｅ　Ｓｙｓｔｅｍｓ　Ｌｔｄ．社のＨＡＳＰ（商標）等がある。
【０００６】以下にプログラム実行制御技術についてより詳細に説明する。
①ソフトウエアの実行を行うユーザはユーザ固有情報として認証鍵を保有する。認証鍵は暗号化のための鍵であり、ソフトウエアの利用を許可する者、例えばソフトウエアベンダーがユーザに配布する。認証鍵は複製を防ぐためにハードウエア中のメモリに厳重に封入され、郵便等の物理的手段を用いてユーザに配送される。
②ユーザ認証鍵を内蔵したハードウエアを指定された方法で所有者のパソコンまたはワークステーションに装着する。ハードウエアは例えばプリンタポート等に装着される。
③ユーザがアプリケーションプログラムを起動し、プログラムの実行が前記アクセス資格認証ルーチンに及ぶと、プログラムはユーザの認証鍵を内蔵したハードウエアと通信する。通信結果に基づいてプログラムは認証鍵を識別し、正しい認証鍵の存在が確認されると次のステップへ実行を移す。通信が失敗し認証鍵の存在が確認されない場合は、プログラムは自らを停止し以降の実行ができないようにする。
【０００７】アクセス資格認証ルーチンによる認証鍵の識別は、例えば次のようなプロトコルによって行われる。
①アクセス資格認証ルーチンは適当な数を生成し鍵内蔵ハードウエアに送信する。
②鍵内蔵ハードウエアは内蔵する認証鍵を用いて送られた数を暗号化し、前記アクセス資格認証ルーチンに返信する。
③認証ルーチンは、返信された数が予め予想された数、即ちハードウエアに送信した数を正しい認証鍵で暗号化して得られる数であるか否かを判定する。
④返信された数が予想された数と一致する場合にはプログラムの実行を継続し、一致しない場合にはプログラムを停止する。
【０００８】この際のアプリケーションプログラムと認証鍵内蔵ハードウエア間の通信は、たとえ同じアプリケーションプログラム中の同じ箇所において同じハードウエアとの間で交換されるものであろうとも、実行のたびに異ならなければならない。さもなければ、正常な実行過程における通信内容を一度記録し、以後プログラムを実行するたびに記録した通信内容をアプリケーションプログラムに返信することにより、正しい認証鍵を保有しないユーザでもプログラムを実行することが可能となってしまう。このような攻撃をリプレイアタックと呼ぶ。
【０００９】リプレイアタックを防ぐために、通常鍵内蔵ハードウエアに送られる数は通信のたびに新たに生成される乱数を用いる。

【００１０】〔従来技術の問題点〕従来技術の問題点は、アプリケーションプログラムを作成する際に、プログラム作成者がユーザが持つ認証鍵を予め想定した上で、該認証鍵に基づいてプログラムの保護処理を行わなければならないという性質に由来する。

【００１１】つまり、プログラムの作成者は、鍵内蔵ハードウエアからの正しい返信をプログラム作成時に予側して、正しい返信を受けた場合にのみプログラムが正常に実行されるようにプログラムの作成を行わなければならない。

【００１２】前記の特徴を有する従来技術の利用形態は基本的に前記の二通りとなるが、いずれの場合も以下に述べる問題を有する。

【００１３】①第１の方法では、ユーザの認証鍵をユーザ毎に異なるように用意する。即ち、ユーザ甲には認証鍵甲、ユーザ乙には認証鍵乙というように、ユーザごとに異なる認証鍵を１つずつ用意する。この場合、プログラム中の認証ルーチンは該プログラムを利用するユーザの固有の認証鍵を認証できるように作成されなければならず、プログラム作成者は利用ユーザの数だけ異なるプログラムを作成する必要がある。

【００１４】対象となるユーザが多数の場合、プログラムをユーザ毎にカスタマイズ（個別化）する作業はプログラム作成者にとって耐え難い労力を要求し、管理しなければならないユーザ認証鍵のリストも膨大なものとなる。

【００１５】②第２の方法では、プログラムの作成者はアプリケーションごとにそれぞれ異なる認証鍵を用意する。即ち、アプリケーション甲には認証鍵甲、アプリケーション乙には認証鍵乙というように、アプリケーションごとに異なる認証鍵を１つずつ用意し、固有の認証鍵を識別するように各アプリケーションプログラムを作成する。

【００１６】この方法では、第１の方法のようにユーザ毎にプログラムを個別的に作成する必要はなくなるが、逆にユーザは利用するアプリケーションの数だけ認証鍵を保持しなければならないことになる。

【００１７】上述のように、認証鍵はハードウエアに厳重に封入した状態でユーザに配布する必要がある。従って、プログラム自身はネットワークを介して簡便に配布することができるのに対し、認証鍵を内蔵するハードウエアの配布は郵便等の物理的手段に頼らざるを得ない。プログラム作成者はユーザからのアプリケーションの使用許諾以来を上け取るたびに、そのアプリケーションに対応する認証鍵が封入されたハードウエアを郵送する必要があり、コスト、時間、梱包の手間いずれをとってもプログラム作成者にとって大きな負担となる。

【００１８】また、ユーザは利用するアプリケーションを変更するたびにハードウエアを交換しなければならないという煩雑さに甘んじなければならない。

【００１９】ユーザがあるアプリケーションを使いたいとしても、認証鍵が封入されたハードウエアが郵送されて到着するまで待たなければならず、即座に利用できないという問題もある。

【００２０】これら問題を軽減するために、ハードウエア中に予め複数の認証鍵を封入しておき、新しいアプリケーションの利用をユーザに許可するたびに、ハードウエア中の認証鍵を利用可能とするためのパスワードをユーザに教えるという方法を用いることはできるが、予め封入された認証鍵を使い切った場合は同様の問題が発生し、本質的な解決とはなっていない。

【００２１】前記のような実効制御の方法以外に、単にアプリケーションを暗号化して、その復号鍵を安全な方法でユーザに教えるという単純な方法が一般的に広く用いられているが、この方法では、アプリケーションを一旦復号してしまうと、ユーザは好きなようにアプリケーションをコピーして不正に配ることができるため、ほとんど防御されていないとみなしてよい。

【００２２】従って、デジタル化された情報、例えばソフトウエア、音楽、映画等（以後これらを総称してコンテンツと呼ぶ）をネットワークで配送して、正当な対価を得ようとした場合、従来の技術では、コンテンツの管理が煩雑になったり、認証用のハードウエアの管理でユーザに大きな負担をかけてしまうという問題があった。

【００２３】

【発明が解決しようとする課題】本発明は、このような問題に鑑みなされたものであり、ユーザおよびサービス提供者の負担を最小限に押さえながら、サービスの利用を正当な権利を有するユーザにのみ提供することができるシステム、または、サービスの利用に応じた正当な対価を回収することが可能なシステムを提供することを目的とする。

【００２４】

【課題を解決するための手段】本発明の第１の側面によれば、上述の目的を達成するために、正当な権利を有するユーザのみにサービスを提供するサービス提供装置に、認証用データを記憶する第１の記憶手段と、ユーザの固有情報を記憶する第２の記憶手段と、前記ユーザの固有情報と、アクセス資格認証の特徴情報とに対し、所定の計算を実行した実行結果である証明用補助情報を記憶する第３の記憶手段と、前記第１の記憶手段に保持されている認証用データと、前記第２の記憶手段に記憶されている前記ユーザの固有情報と、前記第３の記憶手段に記憶されている前記証明用補助情報とに所定の計算を施して証明データを生成する証明データ生成手段とを設けるようにしている。

【００２５】また、本発明の第２の側面によれば、正当な権利を有するユーザのみにサービスを提供するサービス提供装置に、認証用データを記憶する第１の記憶手段と、ユーザの固有情報を記憶する第２の記憶手段と、前

記ユーザの固有情報と、アクセス資格認証の特徴情報とに対し、所定の計算を実行した実行結果である証明用補助情報を記憶する第３の記憶手段と、前記第１の記憶手段に保持されている認証用データと、前記第２の記憶手段に記憶されている前記ユーザの固有情報と、前記第３の記憶手段に記憶されている前記証明用補助情報とに所定の計算を施して証明データを生成する証明データ生成手段と、前記証明データ生成手段によって生成された証明データが前記アクセス資格認証の特徴情報に基づいて生成されていることを検証する証明データ検証手段とを設けるようにしている。

【００２６】これらの構成によれば、証明用補助データ（アクセスチケット）を導入することにより、プロテクト側で付与されるアクセス資格認証用の特徴情報とユーザ側に付与されるユーザ固有情報とを独立させることができ、ユーザは予めユーザ固有情報を所持し、プログラム作成者等のプロテクト者はユーザが所持するユーザ固有情報とは独立にアクセス資格認証の特徴情報を用いてアプリケーションプログラムを作成し、その後、アクセスチケットをユーザの個有情報とアプリケーションプログラムの作成等に使用したアクセスチケット資格認証の特徴情報とに応じて作成し、配布することにより、実行制御等のユーザアクセス資格の認証を行うことが可能となり、正当な権利を有するユーザにのみ所望のサービスを提供することができる。また、証明データ生成時にログを取るようにすれば、サービスに対する正当な対価を回収することができる。

【００２７】また、前記の構成においては、少なくとも前記第２の記憶手段と、前記証明データ生成手段とが、内部データおよび処理手続きを外部から観測することが困難ならしめる防御手段中に保持されるようにしてもよい。

【００２８】また、前記の構成においては、少なくとも前記証明データ検証手段が、内部データおよび処理手続きを外部から観測することが困難ならしめる防御手段中に保持されるようにしてもよい。

【００２９】また、前記アクセス資格認証の特徴情報が暗号化関数における復号鍵であり、前記認証用データが適当なデータを前記復号鍵に対応する暗号化鍵を用いて暗号化したものであり、前記証明データ検証手段により、前記証明データ生成手段が生成する証明データが前記認証用データを正しく復号したものであることを検証するようにしてもよい。また、前記アクセス資格認証の特徴情報が暗号化関数における暗号化鍵であり、前記認証用データが適当なデータを前記暗号化鍵に対応する復号鍵を用いて復号したものであり、前記証明データ検証手段により、前記証明データ生成手段が生成する証明データが前記認証用データを正しく暗号化したものであることを検証するようにしてもよい。また、前記アクセス資格認証の特徴情報がデジタル署名関数における署名鍵であり、前記証明データ生成手段が生成する証明データが、前記認証用データに対して、前記署名鍵を用いて正しく生成されたデジタル署名であることを検証するようにしてもよい。

【００３０】また、前記アクセス資格認証の特徴情報が暗号化関数における第１の復号鍵であり、前記認証用データが前記暗号化された情報を復号する第２の復号鍵を前記第１の復号鍵に対応する暗号化鍵を用いて暗号化したものであり、前記証明データ生成手段によって生成された証明データが前記第２の復号鍵であり、前記第２の復号鍵を用いて前記暗号化された情報を復号して、前記情報に対応するサービスを提供するようにしてもよい。また、前記暗号化関数が非対称鍵暗号化関数であり、アクセス資格認証の特徴情報が鍵の一方であってもよい。

【００３１】また、前記暗号化関数が公開鍵暗号化関数であり、アクセス資格認証の特徴情報が秘密鍵であってもよい。

【００３２】また、前記暗号化関数が対称鍵暗号化関数であり、アクセス資格認証の特徴情報が共通秘密鍵であってもよい。

【００３３】また、前記第１の記憶手段と、前記第２の記憶手段と、前記第３の記憶手段と、前記証明データ生成手段とから構成される証明データ生成装置と、前記証明データ検証手段に加え、認証用データを記憶する第４の記憶手段と、証明データを記憶する第５の記憶手段をそなえた証明データ検証装置とが、互いに通信することによりユーザのアクセス資格を認証するアクセス資格認証装置を有するサービス提供装置において、証明データ検証装置は、第４の記憶手段に記憶されている認証用データを証明データ生成装置の第１の記憶手段に書き出し、証明データ生成装置は、証明データ生成手段によって第１の記憶手段に書き込まれた前記認証用データをもとに生成した証明データを、証明データ検証装置中の第５の記憶手段にかき出し、証明データ検証装置は第５の記憶手段に書き込まれた前記証明データを用いてユーザのアクセス資格を認証するようにすることもできる。

【００３４】また、アクセス資格認証用の特徴情報が暗号化関数の復号鍵であり、証明データ検証装置が乱数生成手段と、生成した乱数を記憶する第６の記憶手段と、認証用素データを記憶する第７の記憶手段とを備え、乱数生成手段は生成した乱数を第６の記憶手段に書き込むと共に、第７の記憶手段に記憶されている認証用素データに前記乱数を用いた乱数効果を施した後、認証用データとして第４の記憶手段に書き込み、証明データ検証手段は、第６の記憶手段に記憶されている乱数による乱数効果を、前記証明データ生成装置によって第５の記憶手段に書き込まれた証明データから除去した結果が、アクセス資格認証の特徴情報である復号鍵で第７の記憶手段に記憶されている認証用素データを復号したものであることを検証するようにしてもよい。

【００３５】また、アクセス資格認証用の特徴情報が暗号化関数の暗号化鍵であり、証明データ検証装置が乱数生成手段を備え、乱数生成手段は生成した乱数を認証用データとして第４の記憶手段に書き込み、証明データ検証手段は、証明データ生成装置によって第５の記憶手段に書き込まれた証明データが、前記乱数を復号したものであることを検証するようにしてもよい。

【００３６】また、アクセス資格認証用の特徴情報がデジタル署名関数の署名鍵であり、証明データ検証装置が乱数生成手段を備え、乱数生成手段は生成した乱数を認証用データとして第４の記憶手段に書き込み、証明データ検証手段は、証明データ生成装置によって第５の記憶手段に書き込まれた証明データが、前記乱数である認証用データに対する、アクセス資格認証の特徴情報である署名鍵によるデジタル署名であることを検証するようにしてもよい。

【００３７】

【発明の実施の態様】以下、この発明を詳細に説明する。

［実施例１］まず、実施例１を参照して本発明の原理的な構成について説明する。図１は本発明の実施例１の構成を全体として示すものであり、この図１においてサービス提供システムは、証明データ検証装置１０および証明データ生成装置１１からなっており、証明データ生成装置１１はアクセスチケット生成装置１２からアクセスチケット（証明用補助データ）１３を受領するようになっている。証明データ検証装置１０は検証ルーチン１５を実行する。証明データ生成装置１１はユーザ固有情報１６およびアクセスチケット１３を保持し、証明データ生成プログラム１７を実行する。ユーザ固有情報１６および証明データ生成プログラム１７の少なくとも一部が耐タンパー装置２０で保護されている。

【００３８】アクセスチケット生成装置１２はアクセス資格認証の特徴情報１４およびユーザの固有情報１６に基づいてアクセスチケット１３を生成し、アクセスチケット１３はネットワークや記憶媒体等を通してユーザに送られ、ユーザの証明データ生成装置１１に保持される。

【００３９】証明データ検証装置１０は認証用データ１８を証明データ生成装置１１に送信する。証明データ生成装置１１はアクセスチケット１３およびユーザ固有情報１６を用いて証明データ１９を生成し、これを証明データ検証装置１０に返信する。証明データ検証装置１０は認証用データに基づいて証明データの正当性を検証する。即ち、証明データが、検証用データとアクセス資格認証の特徴情報とに基づいて生成されたデータであることを検証する。

【００４０】証明データの正当性が検証されれば、ユーザが正当な権利を有することが認証され、サービス提供装置により所望のサービスが提供される。

【００４１】以下、図２を用い、実際のサービスを例にとって本発明を具体的に説明する。

【００４２】本発明の実施例１では、インターネットブラウザ（Ｎｅｔｓｃａｐｅ　Ｎａｖｉｇａｔｏｒ－米国ネットスケープ・コミュニケーションズ社の商標－等）に、証明データ検証ルーチン１５と復号プログラム３５とを一体化してプラグイン（Ｐｌｕｇ－Ｉｎ）モジュールとして組み込んだ例について述べる。ここで、プラグイン・モジュールとはインターネットブラウザの機能を拡張するソフトウエアプログラムを指し、これにより、ユーザに新しいデータタイプの利用をサポートすることができる。インターネットブラウザがサポートしていないデータタイプの情報をサーバから受け取ると、インターネットブラウザは、そのデータタイプに関連付けられているプラグインを探してロードし、起動する。これにより、ユーザの既存のシステムを変更することなく、シームレスに新しいデータタイプのサポートを可能にするものである。

【００４３】本実施例の場合の新しいデータタイプとは暗号化されたコンテンツ３４を指し、インターネットブラウザが暗号化されたコンテンツ３４をサーバから受け取ると、インターネットブラウザは暗号化されたコンテンツ３４のデータタイプを見て、そのデータタイプに関連付けられているプラグイン３８を探してロードし、起動する。起動されたプラグインは、検証ルーチン１５を起動し、証明用プログラム３２に認証用データを送り、返ってきた証明データを用いて検証を行う。検証ルーチン１５により検証が成功した場合には復号プログラム３５によって、暗号化されたコンテンツ３４が復号されてユーザに提供される。復号されたコンテンツは、ハイパードキュメント、画像、動画、音楽などの情報やダウンロードしたプログラムなどである。

【００４４】証明データ生成装置は、証明用プログラム３２とトークン３３とで構成される。認証用プログラム３２はアクセスチケット１３と認証データ生成プログラムＡ３６を含むソフトウエアプログラムであり、ユーザのパーソナルコンピュータ（ＰＣ）上で動作する。トークン３３は認証データ生成プログラムＢ３７とユーザ固有情報１６とを含み、プローブによる内部状態の窃盗への防御力を有するハードウエア（以下、耐タンパハードウエアと呼ぶ）により構成することが望ましい。なぜならば、ユーザ個有情報は、パスワード認証におけるパスワードに相当するものであり、ユーザの身許を証明する唯一の重要な情報であり、ユーザ固有情報１６を読み出しコピーして配布することができると、正当な権利を持たない者にコンテンツの不正利用を許してしまうことになる。

【００４５】また、ユーザには前記ユーザ固有情報に加え、所定の計算手続きを実行する証明データ生成プログラムＡ、Ｂが与えられる。このプログラムは、プラグイ

ン３８中の検証ルーチン１５と通信を行うためのものであり、ユーザ固有情報１６とアクセスチケット１３が与えられると、認証用データ４２に対して計算を行いユーザの身許を証明する証明データ４５を生成する。この計算の過程でユーザ固有情報１６が用いられるが、上述した理由によりユーザ固有情報１６が外部に漏洩すると問題があるため、ユーザ固有情報を用いる証明データ生成プログラムＢ３７は前記耐タンパハードウエア内に収められる。耐タンパハードウエアとしては、ＩＣカードや樹脂モールド等で保護されたＩＣチップなどが簡便で適用しやすい。しかし、提供するサービスの付加価値が非常に高い場合は、特願平０８－２８４４７５号の「暗号化装置、復号装置、機密データ処理装置、および情報処理装置」で示されるような、高い安全性を有する装置を用いてもよい。

【００４６】証明データ検証ルーチン１５の作用を以下に数例述べる。

【００４７】１．証明データ検証ルーチン１５中には、送信するべきデータ（認証用データ４２）と期待される返信データ（期待値）が埋入されている。証明データ検証ルーチン１５は、前記送信データを取り出してユーザに送信し、ユーザから返信を受け取る。次いで、ユーザからの返信データと前記期待値とを比較して、両者が一致した場合に復号プログラム３５により暗号化されたコンテンツ３４を復号して、ユーザに利用可能な状態でコンテンツを提供する。

【００４８】２．証明データ検証ルーチン１５中には、送信するべきデータと期待される返信データ（期待値）が埋入されている。証明データ検証ルーチン１５は、前記送信データを取り出してユーザに送信し、ユーザから返信を受け取る。次いで、ユーザからの返信データに一方向性関数を施した値を、前記期待値と比較して、両者が一致した場合に復号プログラム３５により暗号化されたコンテンツ３４を復号して、ユーザに利用可能な状態でコンテンツを提供する。

【００４９】上記１，２の作用において、返信データが送信データの所定の暗号化アルゴリズムに従う暗号化の結果であるとした場合には、アクセス資格認証の特徴情報は暗号化鍵となる。また、返信データが送信データの所定の署名アルゴリズムに従うデジタル署名であるとした場合には、アクセス資格認証の特徴情報は署名鍵となる。

【００５０】３．証明データ検証ルーチン１５中には、送信するべきデータが埋入されている。証明データ検証ルーチン１５は、前記送信データを取り出してユーザに送信し、ユーザから返信を受け取る。次いで、前記返信データを復号鍵として、復号プログラム３５により暗号化されたコンテンツ３４を復号して、ユーザに利用可能な状態でコンテンツを提供する。

【００５１】４．証明データ検証ルーチン１５中には、送信するべきデータが埋入されている。証明データ検証ルーチン１５は、前記送信データを取り出して乱数効果を付与した後ユーザに送信し、ユーザから返信を受け取る。次いで、前記返信データから前記乱数効果を取り除いた結果を復号鍵として、復号プログラム３５により暗号化されたコンテンツ３４を復号して、ユーザに利用可能な状態でコンテンツを提供する。

【００５２】５．証明データ検証ルーチン１５は、暗号化されたコンテンツに対応した送信データを受け取る。この場合、送信データは暗号化されたコンテンツの中に埋入されていてもよい。証明データ検証ルーチン１５は、受け取った前記送信データをユーザに送信し、ユーザから返信を受け取る。次いで、前記返信データを復号鍵として、復号プログラム３５により暗号化されたコンテンツ３４を復号して、ユーザに利用可能な状態でコンテンツを提供する。

【００５３】６．証明データ検証ルーチン１５は、暗号化されたコンテンツに対応した送信データを受け取る。この場合、送信データは暗号化されたコンテンツの中に埋入されていてもよい。証明データ検証ルーチン１５は、受け取った前記送信データに乱数効果を付与した後ユーザに送信し、ユーザから返信を受け取る。次いで、前記返信データから前記乱数効果を取り除いた結果を復号鍵として、復号プログラム３５により暗号化されたコンテンツ３４を復号して、ユーザに利用可能な状態でコンテンツを提供する。

【００５４】上記3乃至6の作用において、返信データから正しい復号鍵が得られた場合にかぎって、暗号化されたコンテンツ３４は正しく復号され、ユーザは該コンテンツを利用可能となる。この場合のアクセス資格認証の特徴情報は暗号化された復号鍵を復号するための復号鍵となる。

【００５５】さて、従来の例で述べた実行制御技術では、ユーザ固有情報（ユーザの認証鍵）がアクセス資格認証の特徴情報と同一のものである。従来の証明データ生成ルーチンはアクセス資格認証の特徴情報と証明データ検証ルーチンから送信されたデータとを入力して、返信データを計算する。

【００５６】これに対し本発明の特徴は、ユーザ固有情報１６とアクセス資格認証の特徴情報１４とが互いに独立である点にある。この構成でも、証明データ生成プログラムＡとＢはユーザ固有情報１６と証明データ検証ルーチン１５から送信されたデータ４２に加えて、アクセスチケット１３を入力として返信データ（証明データ）４５を計算する。この構成は以下の性質を持つ。

【００５７】１．アクセスチケット１３は特定のユーザ固有情報１６とアクセス資格認証の特徴情報１４とに基づいて計算されるデータである。

２．ユーザ固有情報１６を知らずにアクセスチケット１３から、アクセス資格認証の特徴情報１４を計算するこ

とは少なくとも計算量的に不可能である。

３．証明データ生成プログラムＡとＢは、ユーザ固有情報１６とアクセスチケット１３とが正しい組み合わせの場合、即ち、ユーザ固有情報１６とアクセスチケット１３との正しい組み合わせが入力された場合に限って、正しい返信データを計算する。

【００５８】以上により、ユーザはあらかじめユーザ固有情報１６を所持し、コンテンツ作成者はユーザが所持するユーザ固有情報１６とは独立にコンテンツを暗号化し、アクセスチケット１３をユーザ固有情報１６とアクセス資格認証の特徴情報とに応じて作成することで、正当な権利を有するユーザにのみユーザ固有情報１６とは独立に暗号化されたコンテンツの利用を享受することができる。

【００５９】また、ユーザ固有情報１６を二つの固有情報からなるものとし、アクセスチケット１３の作成に際して用いる固有情報と、ユーザが通信プログラムにおいて用いる固有情報とを区別して用いることもできる。最も典型的な例は、ユーザ固有情報１６を公開鍵ペアとし、公開鍵を公開固有情報としてアクセスチケット作成に用い、秘密鍵をユーザ個人の秘密固有情報としてトークン３３内に封入しておく方法である。この場合はアクセスチケット１３をアクセス資格認証の特徴情報１４と前記公開鍵ペアの公開鍵から計算できるようにすることにより、秘密鍵であるユーザ固有情報１６を秘密に保ったままアクセスチケット１３を計算することが可能となる。

【００６０】次により具体的な構成について実施例に則して説明する。図２において、インターネットブラウザ３１とプラグイン３８と証明用プログラム３２は、ユーザの用いる計算機３０（ＰＣあるいはワークステーション）上のソフトウエアプログラムとして実現することができる。トークン３３についても同様にソフトウエアプログラムとして実現してもよいが、ユーザを識別するための固有情報（ユーザ固有情報）の安全性を高めるために、該計算機３０に接続される耐タンパ特性を有するトークン３３（ＩＣカード、ＰＣカード、ボード等）を併用するのが望ましい。この際、ＩＣカードのような携帯性を有するハードウエアを用いれば、ユーザが複数のＰＣあるいはワークステーション上で作業する場合に便利である。

【００６１】インターネットブラウザ３１で利用する暗号化されたコンテンツ３４は、ネットワークやＣＤ－ＲＯＭ、ＤＶＤ、フロッピーディスク等の記憶媒体を用いてユーザに供給される。

【００６２】ユーザがインターネットブラウザから暗号化されたコンテンツの利用を要求すると、インターネットブラウザは暗号化されたコンテンツのデータタイプを見て、そのデータタイプに関連付けられているプラグインを探してロードし、起動する。

【００６３】プラグインが起動すると、該プラグイン中の検証プログラムが起動し、証明用プログラム３２と通信してユーザ認証を行い、通信が正しく終了した場合に限って、該コンテンツの復号を実行する。

【００６４】ユーザが暗号化されたコンテンツ３４を利用するためには、ユーザ本人宛に発行されたアクセスチケット（証明用補助情報）を取得する必要がある。ユーザは前記ＰＣあるいはワークステーション上にインストールされた証明用プログラム３２に、取得したアクセスチケットを登録するとともに、例えばユーザ固有情報がＩＣカードに封入されている場合には、ＩＣカードを前記ＰＣあるいはワークステーションに装着する。

【００６５】証明データ生成プログラムＡは、証明データ生成プログラムＢと協調して、ユーザ固有情報１６とアクセスチケット１３とに基づいて計算を行い、その計算に基づいてプラグイン中の検証プログラム１５と通信を行う。

【００６６】通信の結果、検証プログラム１５による認証が成功するのは、ユーザ固有情報と、アクセスチケットと、暗号化されたコンテンツとの３つが正しく対応している場合に限る。ユーザ固有情報あるいはアクセスチケットの一方が欠けていた場合には認証は成功しない。

【００６７】アクセスチケットは特定のユーザ宛に発行される。即ち、アクセスチケットの生成に際して、特定のユーザのユーザ固有情報が使用される。アクセスチケット生成時に使用されるユーザ固有情報と、証明データ生成プログラムによって使用される前記ユーザ固有情報とが一致していない場合、やはり、認証は成功しない。

【００６８】また、アクセスチケットは、特定のアクセス資格認証の特徴情報に基づいて生成され、検証プログラム１５はこのアクセス資格認証の特徴情報を認証するように構成される。従って、アクセスチケットの生成のもととなった特徴情報と、検証プログラム１５が認証しようとする特徴情報とが互いに対応していなかった場合にも、認証は成功しない。

【００６９】アクセスチケットは、それ自身十分な安全性を備えていることから、ネットワークを介して配送することができる。アクセスチケットの安全性とは、以下の二つの性質である。

【００７０】１．アクセスチケットは記名式であり、アクセスチケットが発行されたユーザ本人（正確には、アクセスチケット生成時に用いられたユーザ固有情報の保持者）だけが該アクセスチケットを用いて証明データ生成装置を正しく作動させることができる。従って、悪意の第三者がネットワークを盗聴し、他のユーザのアクセスチケットを不正に手に入れたとしても、この第三者がアクセスチケットの発行先である正規のユーザ固有情報を手に入れない限り、このアクセスチケットを利用することは不可能である。

【００７１】２．アクセスチケットはさらに厳密な安全

性を保持している。即ち、悪意の第三者が任意の個数のアクセスチケットを集めて、いかなる解析を行ったとしても、得られた情報をもとに別のアクセスチケットを偽造したり、証明データ生成装置の動作を模倣して認証を成立させるような装置を構成することは不可能である。

【００７２】実施例１では、アクセスチケットｔは次の式１に基づいて生成されるデータである。

【００７３】

【数１】

（１）　ｔ＝Ｄ－ｅ＋ωϕ（ｎ）

上式中の記号はすべて整数であり、以下を表す。ｎはＲＳＡ（Ｒｉｖｅｓｔ－Ｓｈａｍｉｒ－Ａｄｅｌｍａｎ）法数、即ち十分大きな二つの素数ｐ、ｑの積である（ｎ＝ｐｑ）。ϕ（ｎ）はｎのオイラー数、即ち、ｐ－１とｑ－１の積である（ϕ（ｎ）＝（ｐ－１）（ｑ－１））。ｅはユーザ固有情報を表し、ユーザ毎に異なる数で、ユーザを識別するために用いる。Ｄはアクセスチケット秘密鍵すなわちアクセス資格認証の特徴情報を表し、法数ｎのもとでのＲＳＡ秘密鍵であり、式２を満たす。

【００７４】

【数２】（２）　ｇｃｄ（Ｄ，ϕ（ｎ））＝１

ここで、ｇｃｄ（ｘ，ｙ）は二数ｘ、ｙの最大公約数を表す。式（２）によって表現される性質は、式３を満たす数Ｅが存在することを保証する。

【００７５】

【数３】（３）　ＥＤ　ｍｏｄ　ϕ（ｎ）＝１

Ｅをアクセスチケット公開鍵と呼ぶ。

【００７６】ωは、ｎおよびｅに依存して定まる数であり、ｎあるいはｅのいずれか一方が異なる場合、その値が容易に一致しない（衝突しない）ように定める。ωの定め方の一例として、一方向性ハッシュ関数ｈを利用して、式４のようにωを定める方法もある。

【００７７】

【数４】（４）　ω＝ｈ（ｎ｜ｅ）

ただし、記号｜はビット列の結合を表す。

【００７８】一方向性ハッシュ関数とは、ｈ（ｘ）＝ｈ（ｙ）を満たす相異なるｘ、ｙを算出することが著しく困難であるという性質を持つ関数である。一方向性ハッシュ関数の例として、ＲＳＡ　Ｄａｔａ　Ｓｅｃｕｒｉｔｙ　Ｉｎｃ．によるＭＤ２、ＭＤ４、ＭＤ５、および米国連邦政府による規格ＳＨＳ（Ｓｅｃｕｒｅ　Ｈａｓｈ　Ｓｔａｎｄａｒｄ）が知られている。

【００７９】上記の説明中に現れた数において、ｔ、Ｅおよびｎは公開可能であり、残りのＤ、ｅ、ω、ｐ、ｑおよびϕ（ｎ）はチケットを作成する権利を有する者以外には秘密である必要がある。

【００８０】図３に、ユーザが用いる計算機（ＰＣあるいはワークステーション）の概略図を示す。図３においては、ユーザが用いる計算機３０に、カードリーダ３９が接続されており、ユーザはカードリーダ３９にトークン３３を挿入して利用する。インターネットブラウザ３１、プラグイン、証明用プログラムは、計算機３０上のソフトウエアプログラムとして実現されている。また、アクセスチケットも計算機３０の記憶領域に記憶されている。今、利用しようとしているコンテンツは、ヨットの絵の画像であり、正当なトークンと正当なアクセスチケットを持つユーザが、暗号化されたコンテンツをインターネットブラウザ３１に読み込ませると、図３に示すようにプラグインによってインターネットブラウザ３１上に、ヨットの絵の画像が表示される。

【００８１】図４を参照してさらに実施例１について詳細に説明する。図４は、本発明の実施例１の構成例を具体的に示すものである。図２と対比させると検証ルーチン１５に対応するものは、アクセスチケット公開鍵記憶部５１、認証データ記憶部５２、乱数発生部５３、乱数記憶部５４、送信データ（チャレンジ）計算部５５、データ分離部５６、証明データ受信部５７、乱数効果除去部５８、および検証部５９とで構成され、復号プログラム３５は、復号／表示部６１に対応する。この例では検証ルーチンと復号プログラムとを分けて構成してあるが、必要に応じて復号プログラムを検証ルーチンに併合させてもよい。また、証明用プログラム３２は、認証用データ受信部７１、アクセスチケット記憶部７２、第１演算部７３および証明データ生成部７６とで構成され、トークン３３はユーザ固有情報記憶部７４および第２演算部７５とで構成される。

【００８２】次に、動作について説明する。以下の説明における変数は、すべて整数である。

【００８３】［ステップ１］：ユーザがインターネットブラウザから暗号化されたコンテンツの利用を要求すると、インターネットブラウザは暗号化されたコンテンツのデータタイプを見て、そのデータタイプに関連付けられているプラグインを探してロードし、起動する。対応するプラグインが起動すると、プラグイン中の検証ルーチン１５が立ち上がる。この場合のコンテンツとはユーザがインターネットブラウザを通して利用するようなものを指し、例えばホームページの表示情報（画像、動画、ハイパードキュメントなど）であったり、Ｊａｖａアプレットのようなプログラムであったりする。

【００８４】［ステップ２］：プラグインの検証ルーチン１５は、データ分離部において暗号化されたコンテンツからアクセスチケット公開鍵（Ｅ，ｎ）と認証データK^Eを取り出し、それぞれアクセスチケット公開鍵記憶部５１と認証データ記憶部５２に格納する。ここでは、該アクセスチケット公開鍵と該認証データは、暗号化されたコンテンツに付随して配布されているものとして説明した。このように該アクセスチケット公開鍵と該認証データは、暗号化されたコンテンツに付随していてもよいしネットワークを通して入手できるようにしてもよい

が、安全性を考えると暗号化されたコンテンツに付随しているのが望ましく、さらに、該認証データは、ユーザにはわからないように埋め込まれていることが望ましい。例えば、該認証データは、暗号化してコンテンツの中に埋め込んでおき、取り出したあと、プラグインに持たせた復号鍵で復号するなどの方法を取ればよい。

【００８５】［ステップ３］：次に、検証ルーチン１５は、乱数生成部５３で乱数ｒを生成し乱数記憶部５４に格納し、アクセスチケット公開鍵（Ｅ，ｎ）と認証データK^Eおよび乱数ｒを用いて送信データ（チャレンジ）Ｃを式５に従って計算する。

【００８６】

【数５】（５）　$C = r^E K^E \mod n$

チャレンジＣとアクセスチケット公開鍵法数（ＲＳＡ法数）ｎは、証明データ生成側に送信される。Ｃの値には乱数ｒが含まれているため、通信の度に異なる値となり、リプレイアタックを防止する効果を持つ。

【００８７】［ステップ４］：証明用プログラムでは、検証ルーチンから送られたチャレンジＣとＲＳＡ法数ｎとを認証用データ受信部で受信し、証明データ（レスポンス）Ｒを以下のようにして生成する。まず、第１演算部ではアクセスチケット記憶部７２から、ＲＳＡ法数ｎをキーにして対応するアクセスチケットｔを取得し、ＲＳＡ法数ｎのもとで、式６を実行し中間情報Ｒ’を得る。

【００８８】

【数６】（６）　$R' = C^t \mod n$

［ステップ５］：第２演算部７５は、ユーザ固有情報記憶部７４に記憶されているユーザ固有情報ｅを取得し、式７を実行し差分情報Ｓを得る。

【００８９】

【数７】（７）　$S = C^e \mod n$

［ステップ６］：そして、証明データ生成部７６は第１および第２演算部７３、７５から中間情報Ｒ’および差分情報Ｓを得て、式８の計算を行い証明データＲを得る。

【００９０】

【数８】（８）　$R = R' S \mod n$

証明データＲは、検証ルーチンに送信される。

【００９１】［ステップ７］：検証ルーチン１５の乱数効果除去部５８は、証明データ受信部５７で受信した証明データＲを取得し、乱数記憶部５４に記憶されている乱数ｒとにより、式９の計算を行いＫ’を得る。

【００９２】

【数９】（９）　$K' = R r^{-1} \mod n$

［ステップ８］：検証部５９では、前記乱数効果除去部５８で計算したＫ’がアクセス資格認証の特徴情報であるＤに基づいて生成されていることを検証する。Ｋ’が正しくアクセス資格認証の特徴情報であるＤに基づいて生成されている場合には、Ｋ’＝Ｋが成り立つはずである。この式が成り立つかどうかは、このＫ’を用いて暗号化されたデータを復号してみて、正しく復号されるかどうかを判定する方法や、Ｋに冗長性をもたせ、その部分に特定の値を持たせておき、Ｋ’がその特定の値を持っているかどうかで判定する方法などがある。後者の方法には、国際規格ＩＳＯ９７９６などの方法を用いることができる。ここでは、後者の方法を用いて、検証することを前提に説明を続ける。

【００９３】［ステップ９］：検証部５９での検証が正しいと判定されると、検証ルーチンは復号／表示部６１へ復号鍵Ｋ’を渡す。

【００９４】［ステップ１０］：復号／表示部６１は、検証部５９から復号鍵Ｋ’を受け取り、データ分離部５６で分離した暗号化されたコンテンツを復号して表示する。復号されたコンテンツをインターネットブラウザへ渡して、インターネットブラウザで表示する方法も可能であるが、復号された情報がインターネットブラウザによりコピーされる可能性があるため、安全性の面からは、インターネットブラウザが指定した領域にプラグインが直接表示するほうが望ましい。

【００９５】このようにして、正当な権利を有するユーザはインターネットブラウザを用いて暗号化されたコンテンツを利用することができる。このとき、復号されたコンテンツは一時的にしかメモリ上に存在せず、ユーザの利用が終わると消滅するようにすることで、復号されたコンテンツの不正利用を防ぐことができる。

【００９６】本実施例では、暗号化されたコンテンツは、アクセスチケット公開鍵（Ｅ，ｎ）と認証データK^Eとを付随して配布されるものとして説明した。この暗号化されたコンテンツの構成例を図５に示す。図５に示すように、暗号化されたコンテンツは、アクセスチケット公開鍵（Ｅ，ｎ）と、認証データK^Eと、暗号化されたコンテンツ本体とから構成される。検証ルーチンのデータ分離部は、これらを読み込んで、各部分に分離する。

【００９７】コンテンツ本体は鍵Ｋで暗号化されており、認証データK^Eを用いて正しく検証が終了すると、乱数効果除去部を通して鍵Ｋを復元することができ、この鍵Ｋを用いてコンテンツ本体を復号することが可能になる。

【００９８】安全性をより高めるためには、認証データK^Eがユーザには容易に分離できないように埋め込まれていることが望ましい。この実現の一方法を、図６に示す。図６では、図５と同様に、暗号化されたコンテンツは、アクセスチケット公開鍵（Ｅ，ｎ）と認証データK^Eと暗号化されたコンテンツ本体とから構成されるが、コンテンツ本体だけでなく、認証データK^Eもさらに暗号化されている。図６では、認証データK^Eは鍵K_pにより暗号化されているものとして示した。

【００９９】検証ルーチンのデータ分離部は、この暗号

鍵鍵K_Pに対応する復号鍵K_Pを保持しており（共通鍵暗号を用いる例）、入力されたコンテンツ全体から、アクセスチケット公開鍵（E，n）と、暗号化された認証データK^Eと、暗号化されたコンテンツ本体とを分離し、保持している復号鍵K_Pを用いて暗号化された認証データを復号して、認証データK^Eを取り出す。その後、この認証データK^Eを用いて検証を行い、正しく検証が終了すると、乱数効果除去部を通して鍵Kを復元することができ、この鍵Kを用いてコンテンツ本体を復号することが可能になる。

【０１００】ここでは、コンテンツ本体や認証データを暗号化するするのに、共通鍵暗号方式を用いた例を示したため、鍵Kや鍵K_Pは暗号化と復号化とで同じ鍵を用いる例として示したが、この部分をＲＳＡなどの公開鍵暗号方式を用いることも可能である。

【０１０１】また、コンテンツの最も単純な構成例を図７に示す。この例では、コンテンツはコンテンツ本体のみから構成されており、コンテンツ本体も暗号化などの処理が行われていない。しかし、このコンテンツを利用してサービスを提供できるのは特定のプラグインだけであるという状況にある。プラグイン中の検証ルーチンでは、前述したのと同様な処理を行い、検証部における判定の結果、正当であると判断された場合にのみ、プラグインはこのコンテンツを用いてサービスを提供する。

【０１０２】以下では、実施例１において説明した検証ルーチンの検証部における処理の構成例を図８～図１１を用いて数例述べる。図８～図１１では、主に検証ルーチンの中の検証部５９についての構成を示している。ここでは各構成例の違いを明確にするために、検証部５９の中に比較部５９１や期待値記憶部５９２があるような構成として示したが、これに限らず期待値記憶部５９２などは検証部５９の外側に構成しても構わない。

【０１０３】（１）検証部５９の構成例の１を図８に示す。この構成例では、検証部５９は、期待値記憶部５９２と、比較部５９１とを有し、期待値記憶部５９２には証明データとして期待している期待値Ａを記憶している。検証部５９への入力には、証明プログラムから受信した証明データ、あるいは認証データ生成時に乱数効果を付与した場合には受信した証明データから乱数効果を除去した証明データが入力される。この入力された証明データＡ’と、期待値記憶部５９２に記憶している期待値Ａとを比較部５９１で比較する。比較の結果、正当と判定された時には、表示部（復号／表示部６１）に正当の判定を渡し、表示部はデータを表示する。

【０１０４】この構成の場合、期待値記憶部５９２に記憶している期待値Ａがプログラム解析などによって窃取されることは、困難ではあっても不可能ではない。期待値Ａが窃取されると、乱数効果を付与する際の乱数が予想可能であると、証明プログラムの動作を模倣する装置を構成することが可能となり、なりすましによる不正アクセスが可能となる。このようなことを防ぐためには、逆方向への変換が困難な性質を持つ一方向性関数ｈ（）を用いて、期待値記憶部５９２に記憶する期待値として、Ａに一方向性関数ｈ（）を施して得られるデータｈ（Ａ）を記憶しておき、検証部５９１に入力された証明データＡ’に対して、一方向性関数ｈ（）を施した結果のデータｈ（Ａ’）との比較を行うようにすればよい。このように構成することで、万一、期待値記憶部５９２に記憶している期待値ｈ（Ａ）が窃取されたとしても、ｈ（Ａ）からＡを計算することは著しく困難であるので、上記のようななりすましを防ぐことができる。

【０１０５】（２）検証部５９の構成例の２を図９に示す。この構成例では、検証部５９は、期待値記憶部５９２と、比較部５９１と復号鍵記憶部５９３とを有し、期待値記憶部５９２には証明データとして期待している期待値Ａを記憶している。検証部５９への入力には、証明プログラムから受信した証明データ、あるいは認証データ生成時に乱数効果を付与した場合には受信した証明データから乱数効果を除去した証明データが入力される。この入力された証明データＡ’と、期待値記憶部５９２に記憶している期待値Ａとを比較部で比較する。比較の結果、正当と判定された時には、復号鍵記憶部５９３から復号／表示部６１に復号鍵Kを渡し、復号／表示部６１はこの復号鍵Kを用いて暗号化データを復号し、データを表示する。

【０１０６】構成例１と同様に、一方向性関数ｈ（）を用いることも可能である。

【０１０７】（３）検証部５９の構成例の３を図１０に示す。この構成例では、構成例１と同様に検証部５９は、期待値記憶部５９２と、比較部５９１とを有するが、期待値記憶部５９２には期待値として復号鍵Kを記憶している。構成例１と同様に、入力された証明データK’と、期待値記憶部５９２に記憶している期待値Kとを比較部５９１で比較する。比較の結果、正当と判定された時には、復号／表示部６１に復号鍵K’を渡し、復号／表示部６１はこの復号鍵Kを用いて暗号化データを復号し、データを表示する。

【０１０８】（４）検証部５９の構成例の４を図１１に示す。この構成例では、検証部５９は、冗長性検査部５９４を有している。検証部５９への入力には、証明プログラムから受信した証明データ、あるいは認証データ生成時に乱数効果を付与した場合には受信した証明データから乱数効果を除去した証明データが入力される。この入力された証明データK’を冗長性検査部５９４で検査する。この方法は、前述したように予めKに冗長性を持たせておき、K’がその冗長性を持っているかどうかを検査するものである。例えば、国際規格ＩＳＯ９７９６などの方法を用いることができる。冗長性検査部５９４で冗長性の検査に合格すると、冗長性検査部５９４は復号／表示部６１に復号鍵K’を渡し、復号／表示部６１

はこの復号鍵Ｋを用いて暗号化データを復号し、データを表示する。

【０１０９】［実施例２］つぎに本発明の実施例２について説明する。本発明の実施例１では、証明データ生成装置１１によって生成された証明データが検証用データとアクセス資格認証の特徴情報とに基づいて生成されたデータであることを、証明データ検証装置１０の検証ルーチン１５が検証し、証明データの正当性が検証されたときに限って、サービスが提供されるサービス提供装置について、インターネットブラウザに、証明データ検証ルーチン１５と復号プログラム３５とを一体化してプラグイン・モジュールとして組み込んだ例について述べた。実施例１では、検証ルーチン１５が受信した証明データから乱数効果を除去した結果が、復号／表示部により復号するための復号鍵になり、その復号鍵が正当なものであるかどうかを判定して、正当なものであるときのみその復号鍵を用いて、暗号化データを復号してサービスを提供するものであった。

【０１１０】しかし、実施例１のように、証明データから乱数効果を除去した結果を復号鍵として用いる例では、必ずしもその復号鍵の正当性を判定する必要はない。証明データから乱数効果を除去した結果をそのまま復号鍵として用いて、暗号化データを復号することにより、正当な復号鍵である場合には、正しく復号が成功してサービスを提供することが可能になり、正当な復号鍵でない場合には、復号は成功せずに、サービスを提供することができないという結果になるだけである。

【０１１１】実施例２では、このように検証部のない例について説明する。以下、実施例２では、検証ルーチンという言葉は用いるが、この検証ルーチンには検証部は存在しない。つまり、検証が成功したかどうかを判定する部分は存在しない。暗号化されたコンテンツからアクセスチケット公開鍵（Ｅ，ｎ）と認証データK^Eを取り出し、それらを用いて認証用データを生成して証明プログラムに送信し、証明プログラムから返送された証明データから乱数効果を除去した結果を、復号鍵として復号／表示部に渡す処理を行うものである。

【０１１２】図１２は、実施例２の構成例を示したものである。図１２は、図４から検証部５９をなくした構成であり、それ以外は図４と同じ構成である。

【０１１３】動作についても、実施例１で説明したのとほとんど同じであり、［ステップ１］～［ステップ７］は同じ処理を行う。以下、［ステップ８］以降について説明する。

【０１１４】［ステップ８］：ステップ７により検証ルーチンの処理は終了し、検証ルーチンは、前記乱数効果除去部５８で計算したＫ’を復号鍵として復号／表示部６１へ渡す。

【０１１５】［ステップ９］：復号／表示部６１は、検証ルーチンの乱数効果除去部５８から復号鍵Ｋ’を受け取り、データ分離部５６で分離した暗号化されたコンテンツを復号して表示する。証明プログラムにおいて、正当なトークンを持つユーザが正当なアクセスチケットを用いて証明データを生成したときのみ、復号鍵Ｋ’は正しい復号鍵になり、暗号化されたコンテンツが正しく復号されて表示される。トークンまたはアクセスチケットが正当でない時には、復号鍵Ｋ’は正しい復号鍵とはなり得ず、暗号化されたコンテンツは正しく復号されないため、正しい表示がされないことになる。

【０１１６】［実施例３］つぎに本発明の実施例３について説明する。図１３は本発明の実施例３の構成を示している。この実施例３は証明データ検証側で上記とは異なるプロトコルを用いた例であり、実施例１の図８（ｂ）で示した検証部の構成要素を、検証部の外に出した構成に近いものである。図４と対応するものは同じ番号で示してある。図１３において、８１は復号鍵記憶部を表し、コンテンツを復号するための復号鍵Ｋを検証ルーチンが予め保持している。

【０１１７】暗号化されたコンテンツの構成は、暗号化されたコンテンツ本体と、アクセスチケット公開鍵とで構成されており、認証データを含む必要はない。

【０１１８】次に、動作について説明する。以下の説明における変数は、すべて整数である。

【０１１９】［ステップ１］：ユーザがインターネットブラウザから暗号化されたコンテンツの利用を要求すると、インターネットブラウザは暗号化されたコンテンツのデータタイプを見て、そのデータタイプに関連付けられているプラグインを探してロードし、起動する。対応するプラグインが起動すると、プラグイン中の検証ルーチン１５が立ち上がる。この場合のコンテンツとはユーザがインターネットブラウザを通して利用するようなものを指し、例えばホームページの表示情報（画像、動画、ハイパードキュメントなど）であったり、Ｊａｖａアプレットのようなプログラムであったりする。

【０１２０】［ステップ２］：プラグインの検証ルーチン１５は、データ分離部において暗号化されたコンテンツからアクセスチケット公開鍵（Ｅ，ｎ）を取り出し、アクセスチケット公開鍵記憶部５１に格納する。

【０１２１】［ステップ３］：次に、検証ルーチン１５は、乱数生成部５３で乱数ｒを生成し乱数記憶部５４に格納し、乱数ｒを送信データ（チャレンジ）Ｃとして、チャレンジＣとアクセスチケット公開鍵法数（ＲＳＡ法数）ｎとを、証明データ生成側に送信する。この場合、証明用プログラムが返す証明データは、チャレンジＣを法数ｎのもとで、ＲＳＡ暗号を用いて暗号化したものになるはずである。

【０１２２】［ステップ４］：証明用プログラムでは、検証ルーチンから送られたチャレンジＣとＲＳＡ法数ｎとを認証用データ受信部で受信し、証明データ（レスポンス）Ｒを以下のようにして生成する。まず、第１演算

部ではアクセスチケット記憶部７２から、ＲＳＡ法数ｎをキーにして対応するアクセスチケットｔを取得し、ＲＳＡ法数ｎのもとで、式６を実行し中間情報Ｒ’を得る。

【０１２３】［ステップ５］：第２演算部７５は、ユーザ固有情報記憶部７４に記憶されているユーザ固有情報ｅを取得し、式７を実行し差分情報Ｓを得る。

【０１２４】［ステップ６］：そして、証明データ生成部７６は第１および第２演算部７５から中間情報Ｒ’および差分情報Ｓを得て、式８の計算を行い証明データＲを得る。証明データＲは、検証側に送信される。

【０１２５】［ステップ７］：検証ルーチン１５の検証部５９は、受信した証明データＲを取得し、式１０の計算を行い乱数記憶部５４に記憶されている乱数ｒと計算結果ｒ’とを比較することにより検証を行う。

【０１２６】

【数１０】（１０）　$r' = R^{E} \mod n$

乱数ｒと計算結果ｒ’とが等しいとき検証は成功したとみなされ、検証ルーチン１５は復号鍵Ｋを復号／表示部へ渡す。

【０１２７】［ステップ８］：復号／表示部６１は、検証部５９から復号鍵Ｋを受け取り、データ分離部５６で分離した暗号化されたコンテンツを復号して表示する。復号されたコンテンツをインターネットブラウザへ渡して、インターネットブラウザで表示する方法も可能であるが、復号された情報がインターネットブラウザによりコピーされる可能性があるため、安全性の面からは、インターネットブラウザが指定した領域にプラグインが直接表示するほうが望ましい。

【０１２８】このように、検証ルーチンではユーザが正当な権利を有することのみを検証し、検証が成功した場合に、予め登録されていた復号鍵で暗号化されたコンテンツを復号するようにしてもよい。

【０１２９】上記第１ないし実施例３で検証ルーチンの部分をソフトウエアプログラムで構成する例を示したが、その場合、コンテンツの復号鍵Ｋは秘密にしておかなければならない。なぜなら、Ｋが漏洩してしまうと暗号化されたコンテンツは誰でも復号できることになってしまい、コンテンツの不正利用を許してしまうこととなる。従って、検証ルーチンは何らかの方法で内部データを保護する必要がある。そのような方法として、プログラムをマシン語にコード化する際に内部データやプログラム手順が解析し難くなるように難読化する方法がある。これらの技術は、村上隆徳ら「プログラムコードの難読化について」，電子情報通信学会技術研究報告（ＩＥＩＣＥ　Ｔｅｃｈｎｉｃａｌ　Ｒｅｐｏｒｔ）情報セキュリティ，ＩＳＥＣ９５－２５（１９９５）等で紹介されている。また、ソフトウエア的手法以外に、検証ルーチンと復号プログラムとを１つのハードウエアで構成する方法を用いてもよい。その場合は、専用のハードウエアやＰＣカードおよびＩＣカード等で構成することができる。また、検証ルーチン、証明データ生成部および復号／表示部すべてを１つのハードウエアで構成することも可能である。

【０１３０】［実施例４］つぎに本発明の実施例４について説明する。本実施例では、利用制御情報を用いた構成例について説明する。利用制御情報は、証明データの生成を制御するための制御情報であり、またサービスを提供する条件を記述する制御情報であり、アクセスチケットとともに配布される。制御情報は、例えば、サービスを提供する期限、料金額、回数、時間などを記述することができ、証明データを生成するときに、これらの条件をチェックして、条件に合致しないときには証明データの生成を行わないようにして、サービスの提供をストップすることができる。これ以外にも制御情報には、役職、性別、年齢などのようなユーザの属性を記述しておいて、トークン中に保持されているユーザの属性と比較して、証明データの生成を制御することも可能である。

【０１３１】以下では、制御情報として利用期限を用いたときの説明と、料金額を用いたときの説明を簡単に述べる。

【０１３２】本実施例では、アクセスチケットｔは次の式１１に基づいて生成されるデータである。

【０１３３】

【数１１】

（１１）　$t = D - F(n, e, L)$

三変数関数Ｆ（ｘ，ｙ，ｚ）は関数値が衝突しにくい三変数関数であり、例えば前述の一方向性ハッシュ関数ｈを利用して式１３のように定めることができる。

【０１３４】

【数１２】

（１２）　$F(x, y, z) = h(x \mid y \mid z)$

上式中の記号はすべて整数であり、実施例１と同様に、ｎはＲＳＡ法数、Ｄはアクセスチケット秘密鍵、ｅはユーザ固有情報を表す。Ｌは利用制御情報であり、関数ＦＯは一方向性関数である。

【０１３５】図１４を参照してさらに本実施例について詳細に説明する。図１４は、本発明の実施例４の構成例を具体的に示すものである。図１４の左半分、つまりプラグインおよび検証ルーチン側は、実施例１の図４と同じである。

【０１３６】証明用プログラム３２は、認証用データ受信部７１、アクセスチケット記憶部７２、第１演算部７３および証明データ生成部７６とで構成され、トークン３３はユーザ固有情報記憶部７４、第２演算部７５および利用制御情報判定部７７とで構成される。

【０１３７】アクセスチケット記憶部７２は、ＲＳＡ法数ｎと、アクセスチケットｔに加えて、利用制御情報Ｌ

とを組にして記憶している。利用制御情報判定部７７は、アクセスチケット記憶部７２から渡された利用制御情報Ｌの条件を判定し、判定の結果正しいと判定したときのみ、利用制御情報Ｌを第２演算部７５に渡す。第２演算部７５では、利用制御情報判定部７７から利用制御情報Ｌを渡されたときのみ、式１３に基づいて差分情報Ｓを計算し、証明データ生成部７６に送る。

【０１３８】

【数１３】

（１３）　$S = C^{F(a,e,L)} \mod n$

以下では、利用制御情報として利用期限を用いたときについて説明する。利用制御情報として利用期限を持つときには、利用制御情報Ｌの値は、例えば１９９７１２３１２４００のような値である。この場合、この値は利用期限が１９９７年１２月３１日２４：００までということを表している。このような数字ではなく、ある日時からの相対的な秒数で表すなどにしてもかまわない。

【０１３９】トークン中の利用制御情報判定部７７は、時計を持ち、アクセスチケット記憶部７２から渡された利用制御情報Ｌと現在の時刻とを比較する。そして比較の結果、利用制御情報Ｌの値が現在の時刻より後である場合には、正しいと判定し、利用制御情報Ｌを第２演算部７５に渡す。第２演算部７５では、利用制御情報判定部７７から利用制御情報Ｌを渡されたときのみ、式１３に基づいて差分情報Ｓを計算し、証明データ生成部７６に送る。

【０１４０】以降、実施例１と同様に、証明データ生成部７６で式８を用いて証明データＲを計算し、検証ルーチン１５の乱数効果除去部５８では、証明データ受信部５７で受信した証明データＲを取得し、乱数記憶部５４に記憶されている乱数ｒとにより、式９の計算を行いＫ’を得る。

【０１４１】正しいアクセスチケットｔと、正しいユーザ固有情報ｅと、正しい利用制御情報Ｌとを用いて計算がなされたときに限って、Ｋ’＝Ｋが成り立ち、検証ルーチン１５の検証部により正しいとの判定が下されて、サービスが提供される。利用制御情報Ｌの利用期限がきれているアクセスチケットを使おうとして、何者かが、アクセスチケット記憶部７２に記憶されている利用制御情報Ｌを改竄したとしても、アクセスチケットｔを改竄することはできないため、証明データ生成部７６で式８を用いて生成された証明データＲは正しい値にはなり得ず、不当にサービスの提供を受けることはできない。

【０１４２】利用制御情報Ｌがサービスの利用額であるときには、例えば利用制御情報Ｌの値として、１回１００円の意味で、１００という数字が与えられている。

【０１４３】トークンは、例えばプリペイドの残高情報を記憶するプリペイド残高記憶部を有し、トークン中の利用制御情報判定部７７は、利用制御情報Ｌとプリペイド残高とを比較して、プリペイド残高の方が大きいときに、正しいと判定し、プリペイド残高から利用制御情報Ｌ分に相当する値を減額して、利用制御情報Ｌを第２演算部７５に渡す。以下の処理は同様である。

【０１４４】また、プリペイド残高記憶部のかわりに、利用履歴記憶部を有し、トークン中の利用制御情報判定部７７は、利用制御情報Ｌの値を時刻などの情報とともに利用履歴記憶部に記録して、利用制御情報Ｌを第２演算部７５に渡すようにしてもよい。この場合には、時々利用履歴記憶部に記憶されている利用履歴を回収して、相当する金額を支払うなどの処理を行う。

【０１４５】このように、ここで示した例以外でも、利用制御情報判定部７７により利用制御情報Ｌをチェックした後で利用制御情報Ｌを第２演算部７５に渡すように構成することで、さまざまな利用制御を行うことが可能になる。

【０１４６】［実施例５］つぎに本発明の実施例５について説明する。実施例５は、衛星放送を利用してカプセル化されたコンテンツを配信して、サービスを提供する例である。ここで、カプセル化とは暗号化等を施すことによりコンテンツをそのままでは利用できないようにすることを指す。図１５に衛星放送を利用したサービス提供システムの概略図を示す。カプセル化されたコンテンツは衛星放送を利用して、各ユーザに配信される。ユーザは衛星電波を衛星アンテナで受信し受信機１００に入力する。受信機では本発明のサービス提供装置が実装してあり、検証が成功した場合にコンテンツを利用できるようになっている。

【０１４７】ここで提供されるコンテンツは、映画、音楽、テレビ番組、ソフトウエア、写真、文献、ニュース等さまざまなものが考えられる。それぞれのコンテンツは受信機１００に接続されたテレビ・ビデオ２００、オーディオ機器３００、コンピュータ（ＰＣ）４００等で利用される。ここでは、受信機１００とサービス利用機器が分割されている例について説明するが、受信機１００が内蔵されたサービス利用機器でも同様に説明できる。

【０１４８】カプセル化されたコンテンツの構造を図１６に示す。カプセル化されたコンテンツは、コンテンツヘッダと暗号化されたデータとに分類される。コンテンツヘッダはコンテンツの識別をするためのラベルと公開鍵（Ｅ，ｎ）および暗号化された復号鍵を有している。暗号化されたデータは前記の実施例で暗号化されたコンテンツ本体に相当する。

【０１４９】図１７は図１５における受信機１００の構成を具体的に示した例である。受信機１００の各回路はマイクロコンピュータによってコントロールされている。衛星アンテナからの衛星信号は、まず受信機１００のチューナ１０１に入力される。チューナ１０１は受信機１００のパネルもしくはリモコンによりユーザが選択したチャネルのデータを抽出する。誤り訂正回路／デス

クランブル回路１０２は、抽出されたデータをコンテンツとして復元し、データ・コントロール回路１０３に入力する。データ・コントロール回路１０３では、コンテンツがカプセル化されているかどうかをコンテンツラベルで識別し、コンテンツがカプセル化されていない場合は、そのまま出力側へ渡す。コンテンツがカプセル化されている場合には、コンテンツを検証／復号回路１０４に入力する。検証／復号回路１０４では、これまでの実施例で示した検証ルーチンにより正当性を検証することが可能であるが、実施例５では、別の方法を示して説明する。この方法の詳細については図１８を参照して説明する。なお、復号されたデータはデマルチプレクス回路１０５を介してビデオデコーダ１０６またはオーディオデコーダ１０７の送られて対応する信号として利用機器に供給される。

【０１５０】図１８に、実施例５の検証手順（プロトコル）を示す。実施例１と同様の機能を有する部分は同じ番号で示してある。

【０１５１】実施例５におけるアクセスチケットｔは式１４に基づいて生成されるデータである。

【０１５２】

【数１４】（１４）　　ｔ＝Ｄ－Ｆ（ｎ，ｅ）

上式中の記号はすべて整数であり、以下を表す。（実施例１の式参照）

ｎはＲＳＡ法数、即ち十分大きな二つの素数ｐ、ｑの積である（ｎ＝ｐｑ）。φ（ｎ）はｎのオイラー数、即ち、ｐ－１とｑ－１の積である（φ（ｎ）＝（ｐ－１）（ｑ－１））。ｅはユーザ固有情報を表し、ユーザ毎に異なる数で、ユーザを識別するために用いる。Ｄはアクセスチケット秘密鍵を表し、法数ｎのもとでのＲＳＡ秘密鍵であり、式２を満たす。ここで、ｇｃｄ（ｘ，ｙ）は二数ｘ、ｙの最大公約数を表す。

【０１５３】式（２）によって表現される性質は、式３を満たす数Ｅが存在することを保証する。Ｅをアクセスチケット公開鍵と呼ぶ。

【０１５４】二変数関数Ｆ（ｘ，ｙ）は関数値が衝突しにくい二変数関数であり、例えば前述の一方向性ハッシュ関数ｈを利用して式１５のように定めることができる。

【０１５５】

【数１５】

（１５）　　Ｆ（ｘ，ｙ）＝ｈ（ｘ｜ｙ）

以下図を用いて、実施例５を詳細に説明する。図１７における検証／復号回路１０４は図１８では３８で示される。検証／復号回路３８は検証ルーチン１５と復号部６１とからなり、ＡＳＩＣ（ａｐｐｌｉｃａｔｉｏｎ ｓｐｅｃｉｆｉｃｉｎｔｅｇｒａｔｅｄ ｃｉｒｃｕｉｔ）等で実現されることで、復号の高速処理や検証ルーチンの安全性が保証される。もちろん検証／復号回路３８をソフトウエアプログラムで実現することも可能である。また、より安全性を高めるために、前述した耐タンパ特性を有するハードウエアで構成してもよい。検証／復号回路では、データ・コントロール回路より受け取ったカプセル化されたコンテンツをデータ分離部５６でコンテンツヘッダと暗号化されたデータとに分離し、公開鍵（Ｅ，ｎ）をアクセスチケット公開鍵記憶部５１に、暗号化された復号鍵K^Eを認証データ記憶部５２に、暗号化されたデータを復号部６１にそれぞれ格納する。そして検証／復号回路は内部の乱数生成部で乱数を生成し乱数記憶部５４に記憶する一方で、送信データ計算部において送信データＣを実施例１と同様に式５に基づいて計算する。

【０１５６】このようにして計算した送信データＣは、法数ｎと一緒に証明プログラムに送信される。

【０１５７】証明プログラムの第１演算部７３および証明データ生成部７６の演算はマイクロコンピュータで実行され、アクセスチケットはＥＰＲＯＭ（ｅｒａｓａｂｌｅｐｒｏｇｒａｍｍａｂｌｅ ｒｅａｄ ｏｎｌｙ ｍｅｍｏｒｙ）等に記憶されている。認証データは受信したｎを基にアクセスチケット記憶部７２から、対応するアクセスチケットｔを選択し、認証データ受信部７１から受け取ったＲＳＡ法数ｎのもとで、式１６を実行し中間情報Ｒ’を得る。

【０１５８】

【数１６】

（１６）　　$R' = C^t \mod n$

トークンはＩＣカードにより実現され、ユーザ固有情報記憶部７４および第２演算部７５を有し、マイクロコンピュータから認証用データを受け取って式１７を実行し差分情報Ｓを得る。

【０１５９】

【数１７】

（１７）　　$S = C^{F(n,e)} \mod n$

そして、証明プログラムの証明データ生成部７５は第１および第２演算部７３、７５から中間情報Ｒ’および差分情報Ｓを得て、式１８の計算を行い証明データＲを得る。

【０１６０】

【数１８】（１８）　　$R = R' S \mod n$

このようにして得られた証明データＲは、検証／復号回路の証明データ受信部５７に送信される。

【０１６１】検証ルーチン１５の乱数効果除去部５８は、データ受信部５７で受信した証明データＲを取得し、乱数記憶部５４に記憶されている乱数ｒとにより、式１９の計算を行い復号鍵Ｋを得る。

【０１６２】

【数１９】（１９）　　$K = R r^{-1} \mod n$

このときＫに冗長性をもたせ、その部分に特定の値を持たせておくことで、復号鍵Ｋが正しく復号されたかどうかを検証部５９で検証するようにしてもよい。得られた

復号鍵Ｋは復号部６１に入力され、復号部６１では暗号化されたデータを復号鍵Ｋを用いて復号しコンテンツとして出力する。

【０１６３】出力されたコンテンツは、デジタルデータとしてＰＣで利用されたり、映像情報やオーディオ情報として利用されたりする。

【０１６４】図１９に、本実施例のサービス提供装置の概観図を示す。図に示すようにサービス提供装置はテレビに接続されている。図には示してないがサービス提供装置は衛星アンテナに接続されており、衛星放送を受信する一方、モデムを通してネットワークに接続されており、衛星放送で受信したカプセル化されたコンテンツを利用するためのアクセスチケットを取得できるようになっている。図１９（ａ）に示すように、コンテンツが暗号化されている場合はトークンをサービス提供装置に挿入していない場合は、ユーザは映像を観ることができない。そこで、ユーザは正当なアクセスチケットを取得してサービス提供装置にトークンを挿入すると、図１９（ｂ）に示すように映像を見ることができるようになる。

【０１６５】このように、本発明では、コンテンツを１つの暗号鍵で暗号化して提供しているにもかかわらず、各ユーザ毎にカスタマイズされたアクセスチケットとユーザ固有情報を格納したトークンを両方有しないとサービスを利用することができないようになっている。従ってコンテンツのプロバイダ（提供者）は、コンテンツを暗号化して衛星放送のようなマスメディアを利用して提供することが可能であり、また、アクセスチケットとトークンとによりユーザごとの確実な利用管理を行うことが可能である。

【０１６６】［実施例６］つぎに本発明の実施例６について説明する。上記はコンテンツごとにカプセル化した場合について記述したが、これ以外の応用例として、衛星放送の放送チャネルについては同じ暗号化を施し、視聴時間を管理することでコンテンツの利用を制限したい場合などがある。このようなサービスはアクセスチケットを式２０で表現することで実現される。

【０１６７】

【数２０】（２０）　　$t = D - F(n, e, L)$

ここで、Ｌは利用制御情報であり、利用期限を表す。三変数関数Ｆ（ｘ，ｙ，ｚ）は関数値が衝突しにくい三変数関数であり、例えば前述の一方向性ハッシュ関数ｈを利用して式２１のように定めることができる。

【０１６８】

【数２１】

（２１）　　$F(x, y, z) = h(x \mid y \mid z)$

図２０に利用制御情報の構成例を示す。図に示すとおり利用制御情報Ｌは利用開始時刻、利用終了時刻および利用料金とで構成される。利用料金はトークンがプリペイド機能を有する場合にのみ必要で、プリペイド機能を使わない場合は省略することができる。図２１に利用制御情報Ｌを用いた場合の検証プロトコルを示す。ここで図１８と同様の機能のものは同じ番号で示してある。

【０１６９】以下、図を用いて実施例６を詳細に説明する。検証／復号回路では、データ・コントロール回路より受け取ったカプセル化されたコンテンツをデータ分離部５６でコンテンツヘッダと暗号化されたデータとに分離し、公開鍵（Ｅ，ｎ）をアクセスチケット公開鍵記憶部５１に、暗号化された復号鍵K^Rを認証データ記憶部５２に、暗号化されたデータを復号部６１にそれぞれ格納する。そして検証／復号回路は内部の乱数生成部で乱数を生成し乱数記憶部５４に記憶する一方で、送信データ計算部において送信データＣを式１５に基づいて計算する。

【０１７０】このようにして計算した送信データＣは、法数ｎと一緒に証明プログラムに送信される。

【０１７１】証明プログラムの第１演算部７３および証明データ生成部７６の演算はマイクロコンピュータで実行され、アクセスチケットはＥＰＲＯＭ（ｅｒａｓａｂｌｅｐｒｏｇｒａｍｍａｂｌｅ　ｒｅａｄ　ｏｎｌｙ　ｍｅｍｏｒｙ）等に記憶されている。認証データは受信したｎを基にアクセスチケット記憶部７２から、対応するアクセスチケットｔと利用制御情報Ｌを選択し、認証データ受信部７１から受け取ったＲＳＡ法数ｎのもとで、式１６を実行し中間情報Ｒ’を得る。

【０１７２】トークンは、ユーザ固有情報記憶部７４、第２演算部７５を有し、さらに、プリペイド度数とトークン時刻データを有している。トークンは、マイクロコンピュータから認証用データと利用制御情報Ｌを受け取り、利用制御情報中の有効期限がトークン時刻と矛盾しないかどうかを検証する。すなわち、利用開始時刻≦トークン時刻≦利用終了時刻となっている場合に検証が成功したとみなされる。有効期限の検証に成功したら、トークンの度数が利用制御情報Ｌ内の利用度数以上残っていることを確認し、残っていればトークンの度数から利用制御情報Ｌ内の利用度数分を減算する。有効期限の検証に失敗した場合と、度数が足りない場合は処理を行わずエラーを返す。上記の検証が成功した場合は、式２２を実行し差分情報Ｓを得る。

【０１７３】

【数２２】

（２２）　　$S = C^{F(0,e,L)} \mod n$

そして、証明プログラムの証明データ生成部７５は第１および第２演算部７３、７５から中間情報Ｒ’および差分情報Ｓを得て、式１８の計算を行い証明データＲを得る。このようにして得られた証明データＲは、検証／復号回路の証明データ受信部５７に送信される。

【０１７４】検証ルーチン１５の乱数効果除去部５８は、データ受信部５７で受信した証明データＲを取得し、乱数記憶部５４に記憶されている乱数ｒとにより、

式１９の計算を行い復号鍵Ｋを得る。ここで、もしトークンで用いた利用制御情報Ｌが改ざんされていた場合は、正確な復号鍵を取り出すことができない。このときＫに冗長性をもたせ、その部分に特定の値を持たせておくことで、復号鍵Ｋが正しく復号されたかどうかを検証部５９で検証するようにしてもよい。得られた復号鍵Ｋは復号部６１に入力され、復号部６１では暗号化されたデータを復号鍵Ｋを用いて復号しコンテンツとして出力する。

【０１７５】出力されたコンテンツは、デジタルデータとしてＰＣで利用されたり、映像情報やオーディオ情報として利用されたりする。

【０１７６】この実施例では、トークンに時刻を持たせているが、ＩＣカードを用いる場合は内部に時計が無いので、トークン時刻の正当性を保証することが必要となる。

【０１７７】このようにすることで、ユーザはアクセスチケットを利用制御情報中の有効期限内でないと利用できず、１つのチャネルのコンテンツが同じ暗号鍵で暗号化してあったとしても、時間毎に利用権を設定することができ、ペイパービュー等の機能を実現することも可能である。

【０１７８】なお、本発明は上述の実施例に限定されるものではなく、例えば、コンテンツの利用は、種々の記録媒体、通信媒体、放送媒体を介して行える。インターネット、衛星放送の他に、種々の通信媒体、放送媒体を利用する場合に適用できる。例えば、通常の電話網、データ通信網、ＴＣＰ／ＩＰ接続による通信カラオケのサービスの提供にも適用できる。

【０１７９】

【発明の効果】以上説明したように、本発明によれば、証明用補助データ（アクセスチケット）を導入することにより、アクセス資格認証の特徴情報とユーザ固有情報とを独立させることができ、従って、プロテクト側も、ユーザ側も１つの固有情報を準備しておけば済む。アクセスチケットは、特定のユーザ固有情報とアクセス資格認証の特徴情報とに基づいて計算されるデータであり、またユーザ固有情報を知らずにアクセスチケットからアクセス資格認証の特徴情報を計算することは少なくとも計算量適に不可能である。そして、ユーザ固有情報とアクセスチケットの正しく組み合わされた場合にのみ、サービスを提供（コンテンツを復号）するので、ユーザは予めユーザ固有情報を所持し、サービス提供者はユーザが所持するユーザ固有情報とは独立にアクセス資格認証の特徴情報を用意することができる。従って、例えばコンテンツを１つの暗号鍵で暗号化した場合でも、所望のユーザだけにアクセス権を設定することが可能となり、暗号化したコンテンツをユーザ毎に用意する必要が無くなる。

【図面の簡単な説明】

【図１】　本発明の原理的な構成例を示すブロック図である。

【図２】　実施例１の構成例の概要を示すブロック図である。

【図３】　実施例１のユーザが用いる計算機の概略図である。

【図４】　実施例１の構成例の詳細なブロック図である。

【図５】　実施例１の暗号化されたコンテンツの構成例１である。

【図６】　実施例１の暗号化されたコンテンツの構成例２である。

【図７】　実施例１の暗号化されたコンテンツの構成例３である。

【図８】　実施例１の検証部における処理の構成例である。

【図９】　実施例１の検証部における処理の構成例である。

【図１０】　実施例１の検証部における処理の構成例である。

【図１１】　実施例１の検証部における処理の構成例である。

【図１２】　実施例２の構成例の詳細なブロック図である。

【図１３】　実施例３の構成例の詳細なブロック図である。

【図１４】　実施例４の構成例の詳細なブロック図である。

【図１５】　実施例５の概略図である。

【図１６】　実施例５のカプセル化されたコンテンツの構成図である。

【図１７】　実施例５の構成例の詳細なブロック図である。

【図１８】　実施例５の構成例の詳細なブロック図である。

【図１９】　実施例５の構成例の図である。

【図２０】　実施例６の利用制御情報の構成図である。

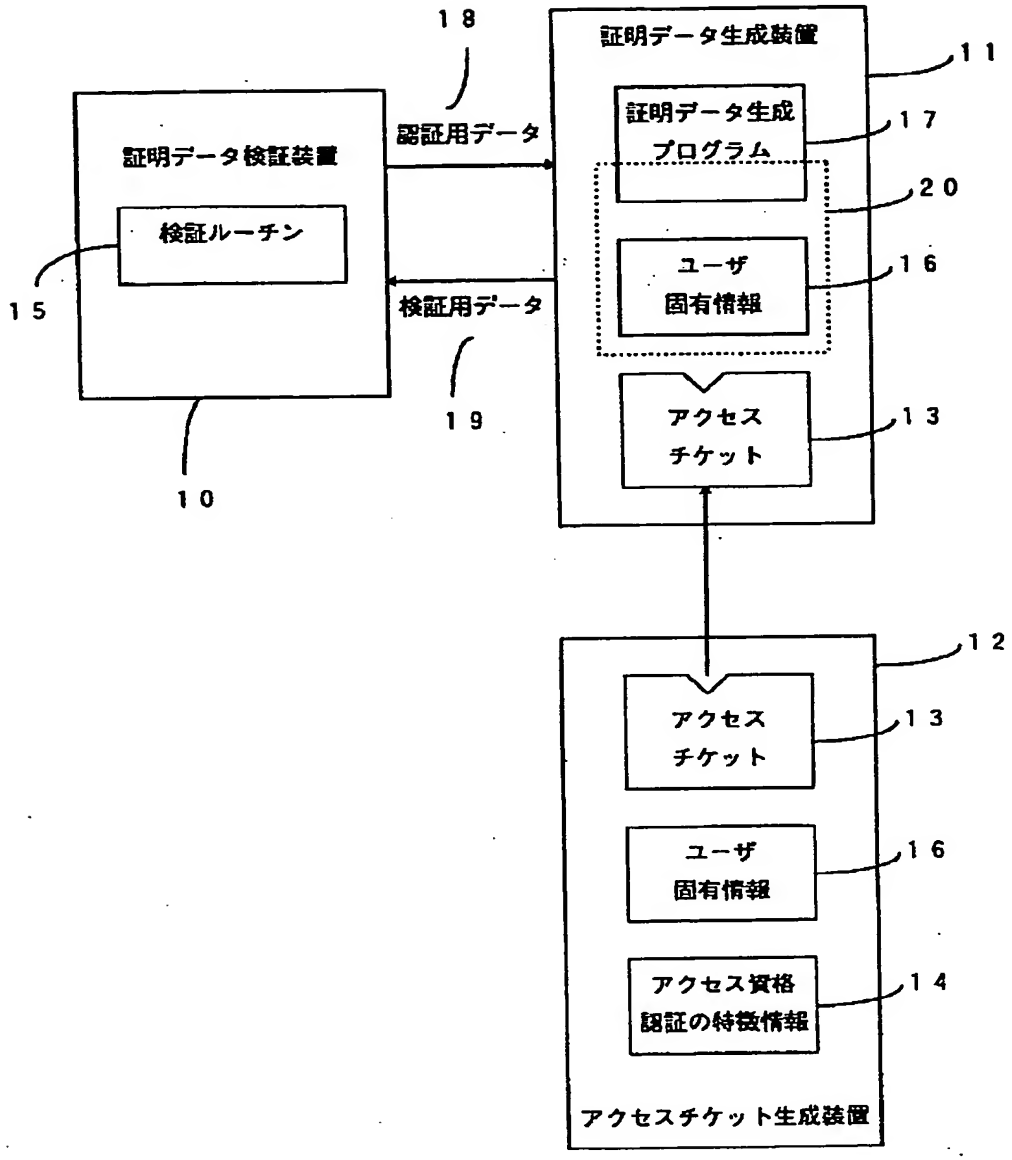
【図２１】　実施例６の構成例の詳細なブロック図である。

【符号の説明】

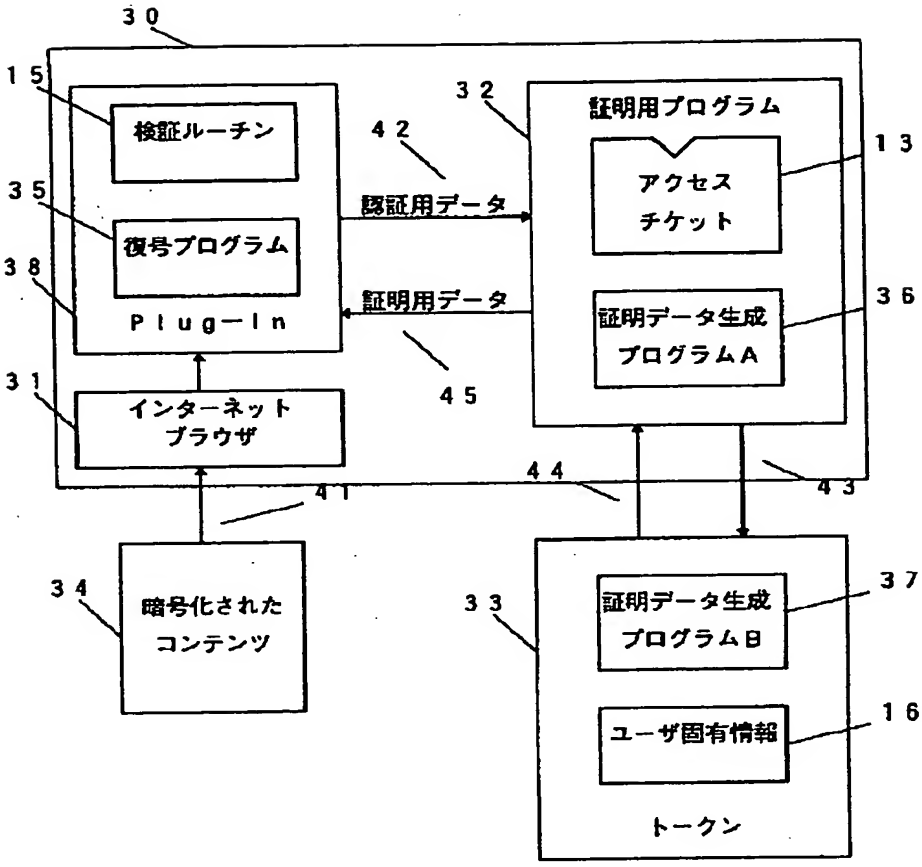
１０　証明データ検証装置
１１　証明データ生成装置
１２　アクセスチケット生成装置
１３　アクセスチケット（証明用補助データ）
１４　アクセス資格認証の特徴情報
１５　検証ルーチン
１６　ユーザ固有情報
１７　証明データ生成プログラム
１８　認証用データ
１９　証明データ

２０　耐タンパー装置
３０　計算機
３１　インターネットブラウザ
３２　証明用プログラム
３３　トークン
３４　コンテンツ
３５　復号プログラム
３８　プラグイン（プラグイン・モジュール）

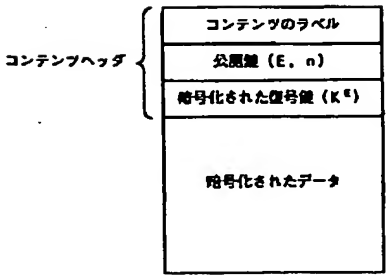
【図１】



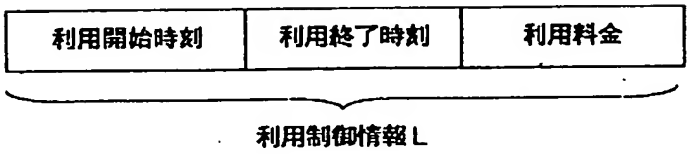
【図２】



【図１４】

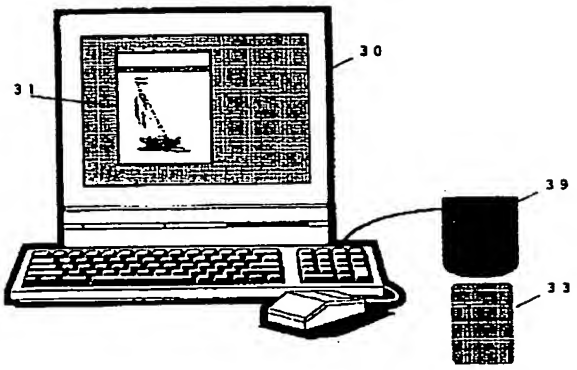


【図１８】

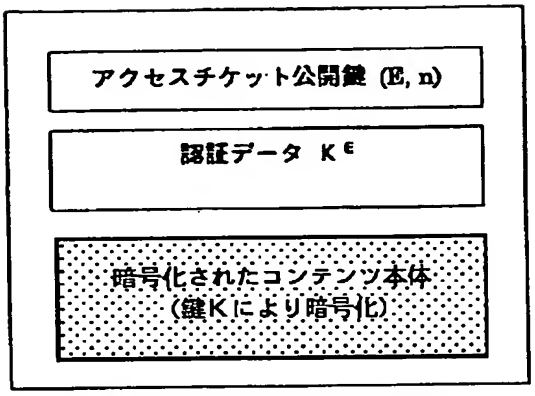


利用制御情報の構成図

【図３】

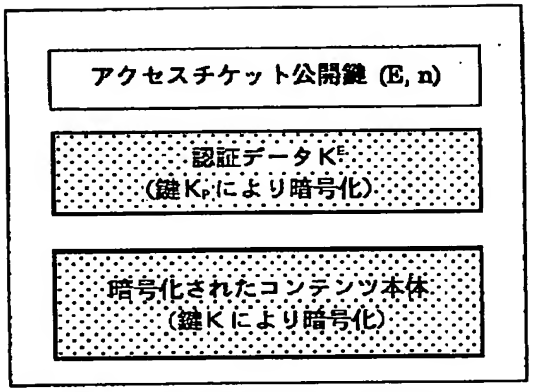


【図５】



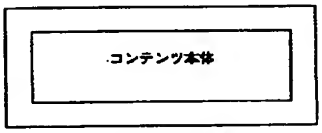
暗号化されたコンテンツの構成１

【図６】



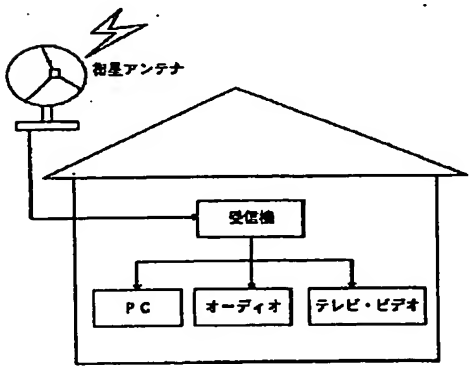
暗号化されたコンテンツの構成２

【図７】

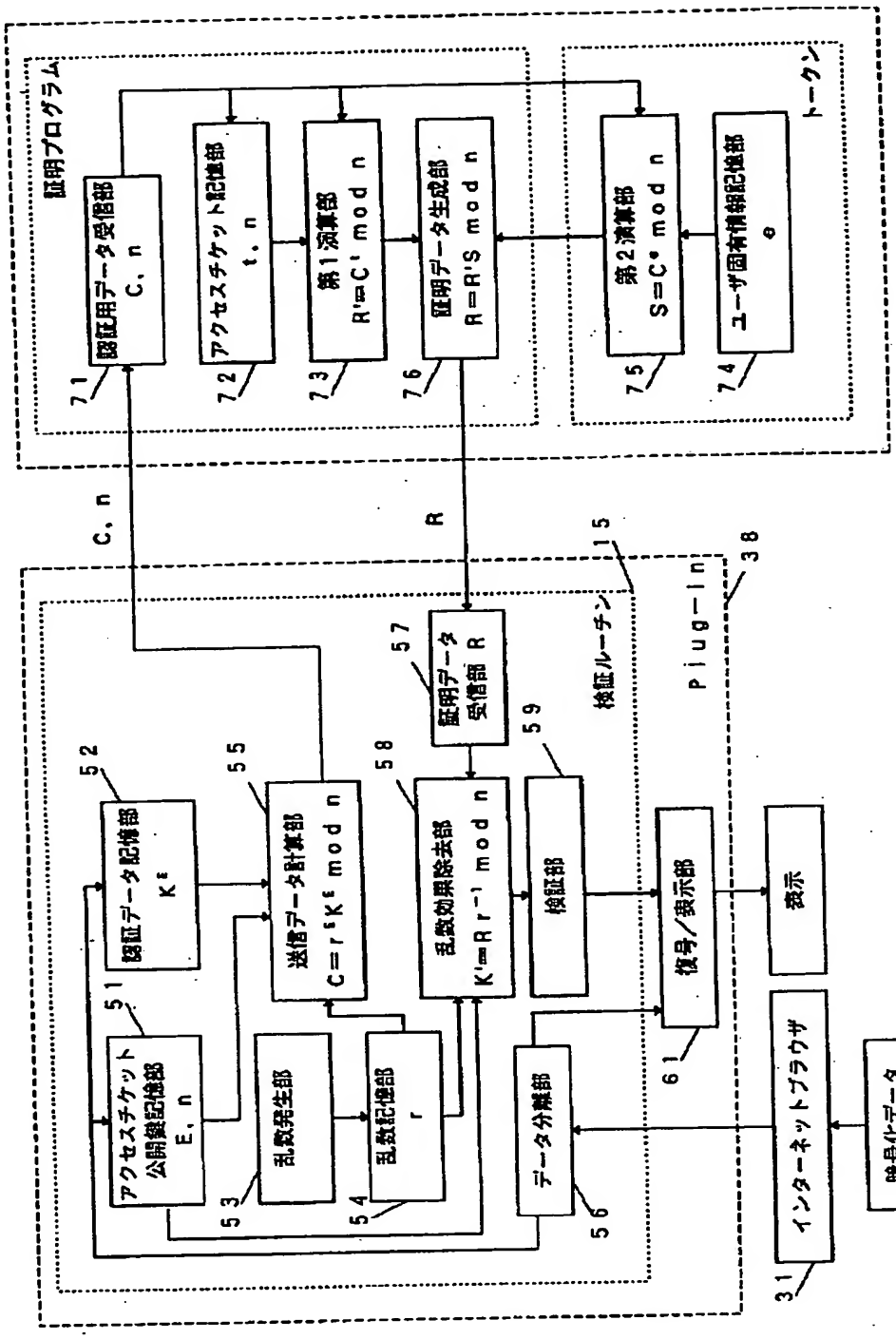


コンテンツの構成３

【図１３】

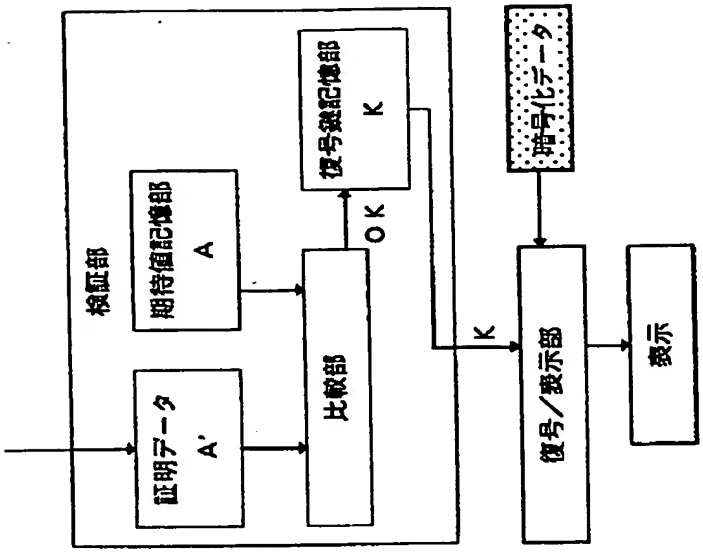


【図4】

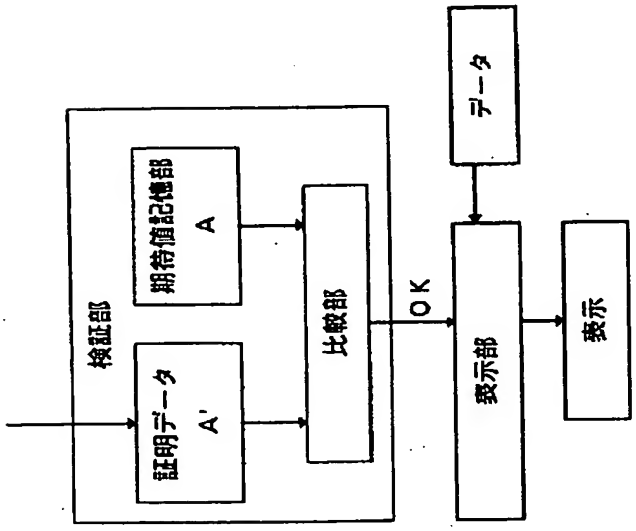


第1の実施例の詳細な構成例

【図８】

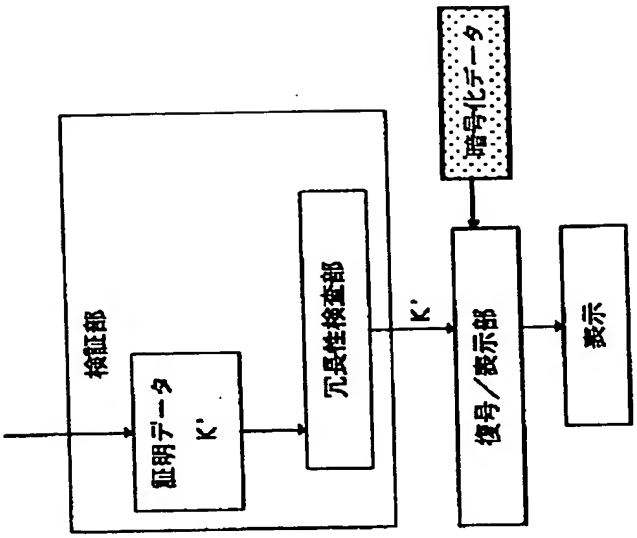


(b) 検証部の構成２

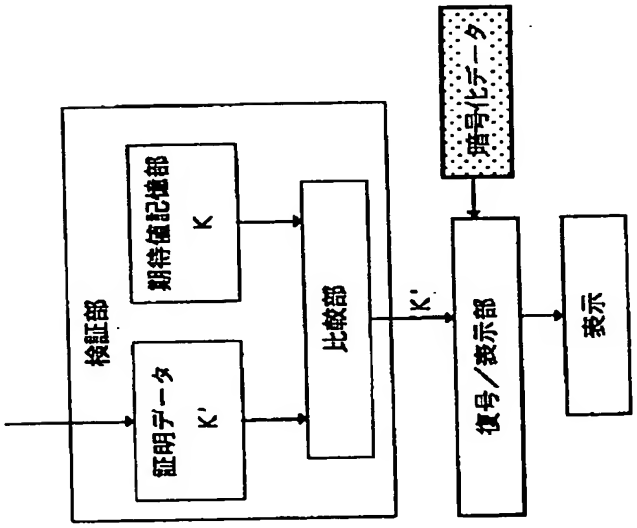


(a) 検証部の構成１

【図９】

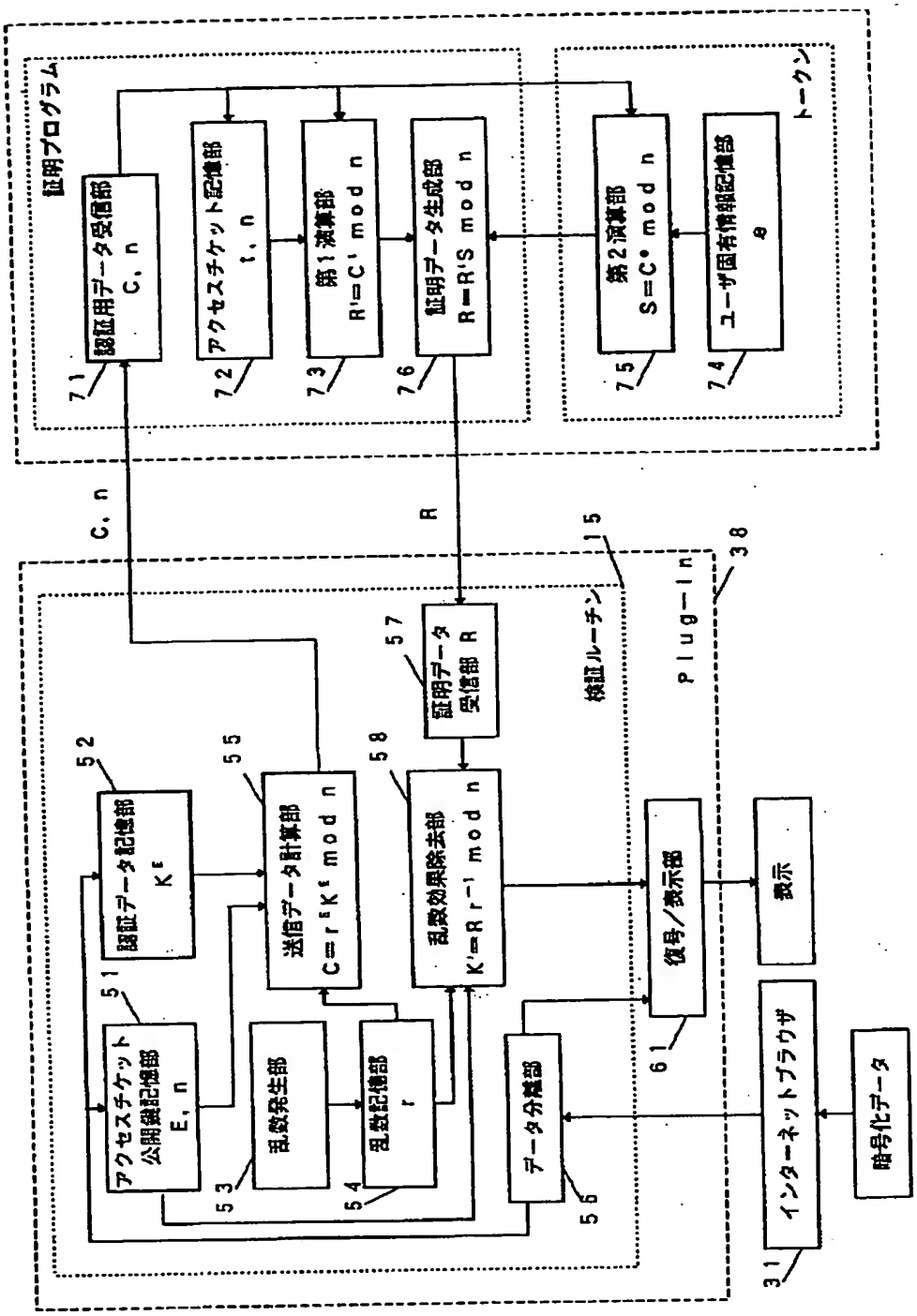


(d) 検証部の構成４



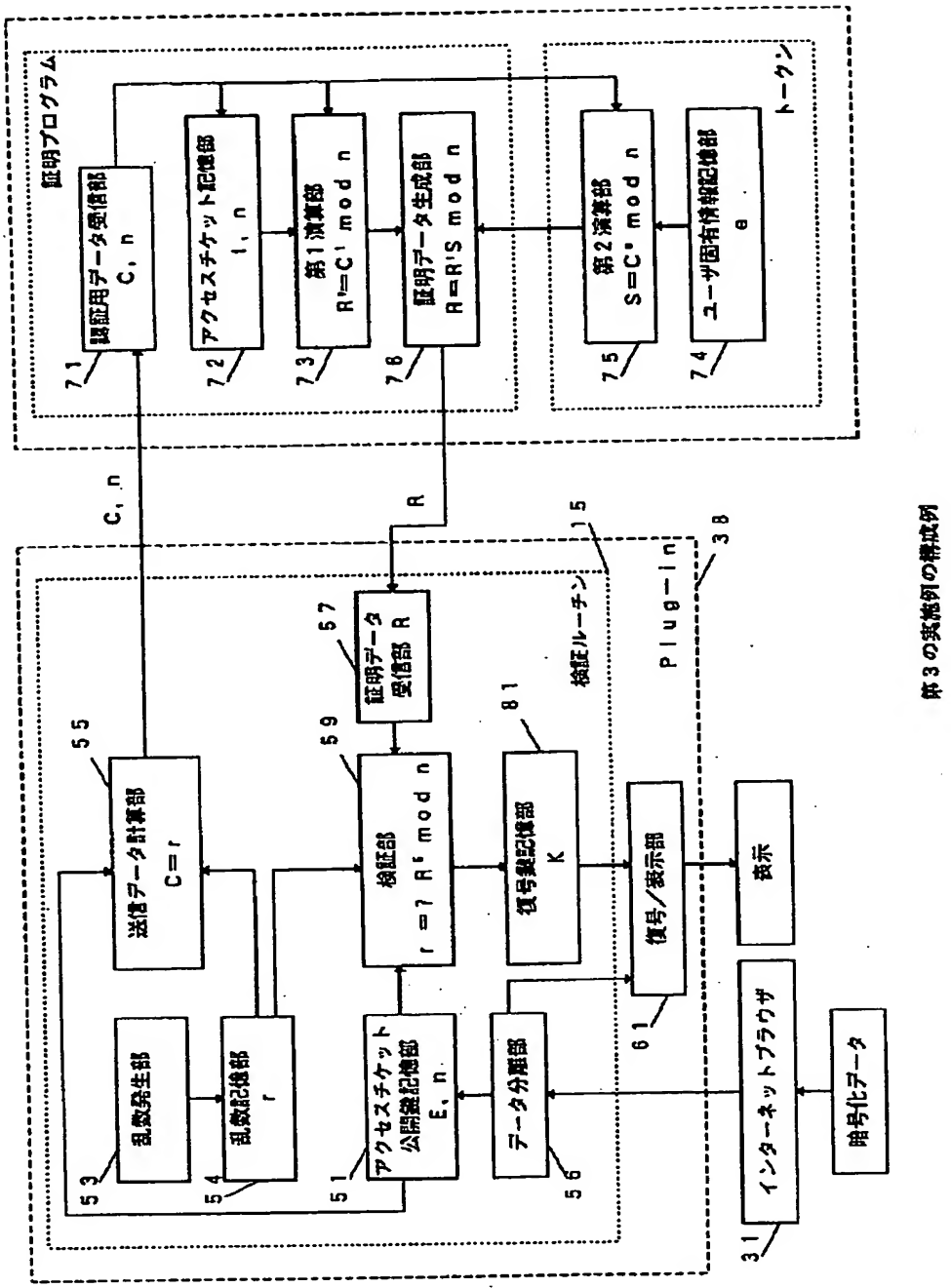
(c) 検証部の構成３

【図１０】



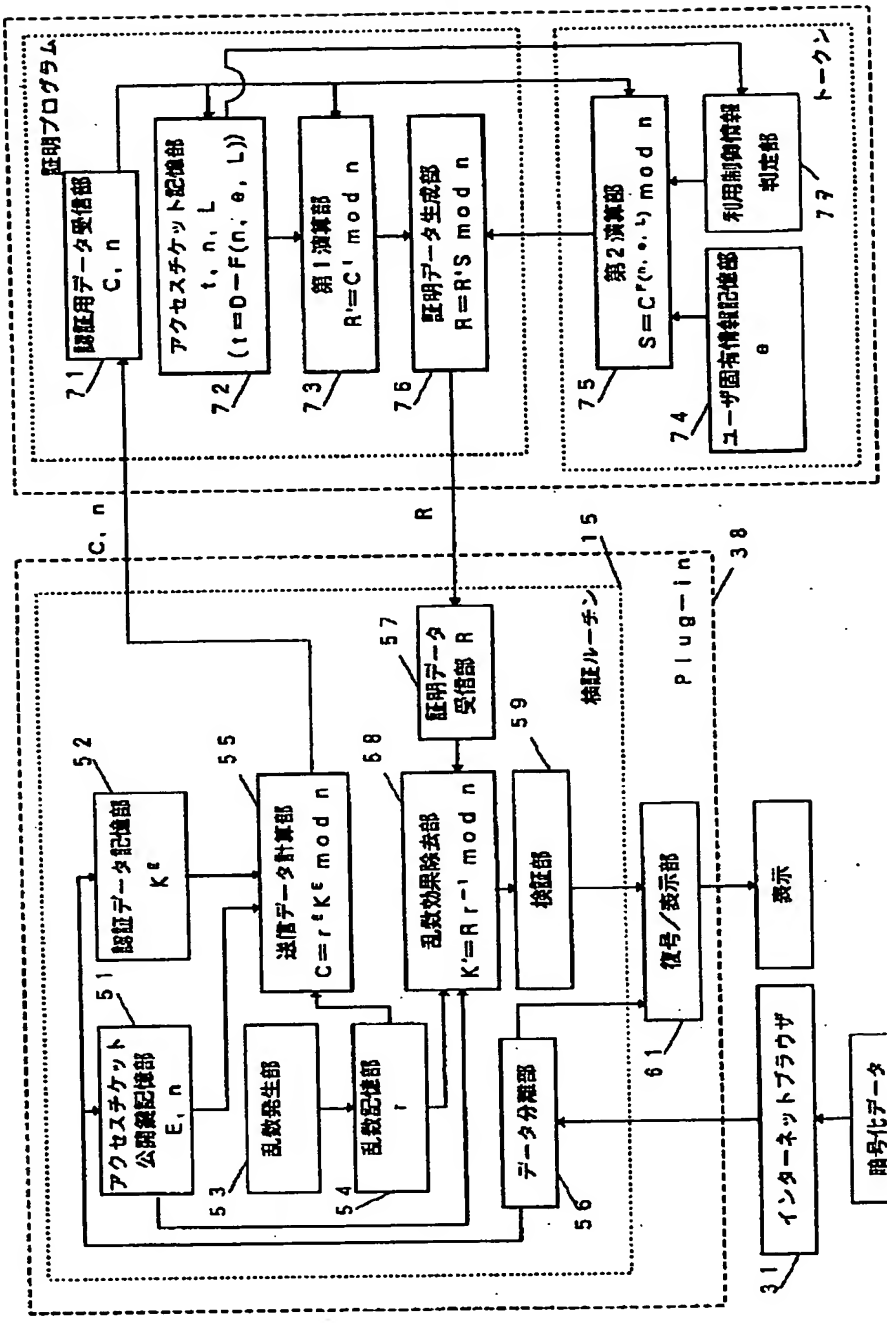
第２の実施例の構成例

【図11】



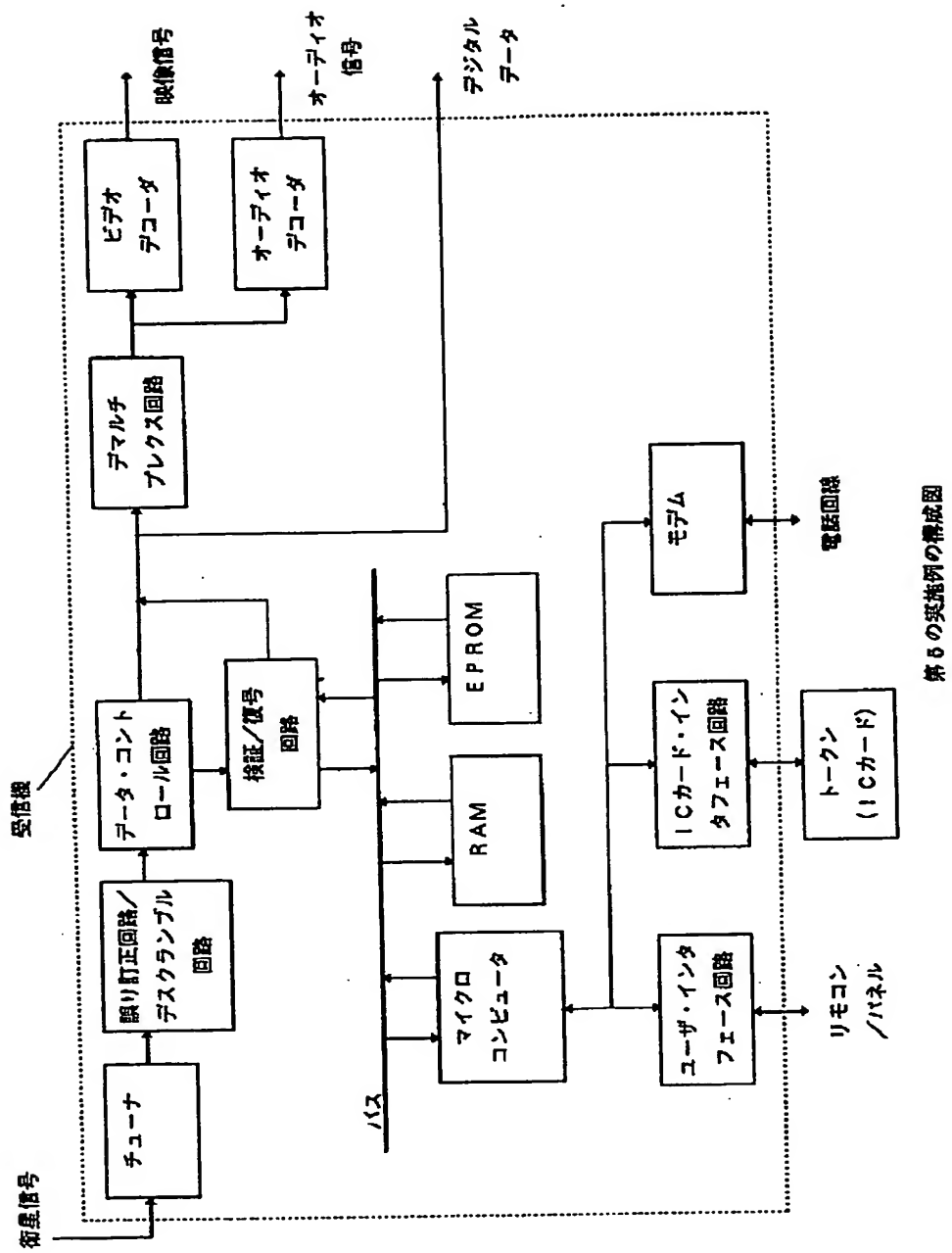
第3の実施例の構成例

【図１２】

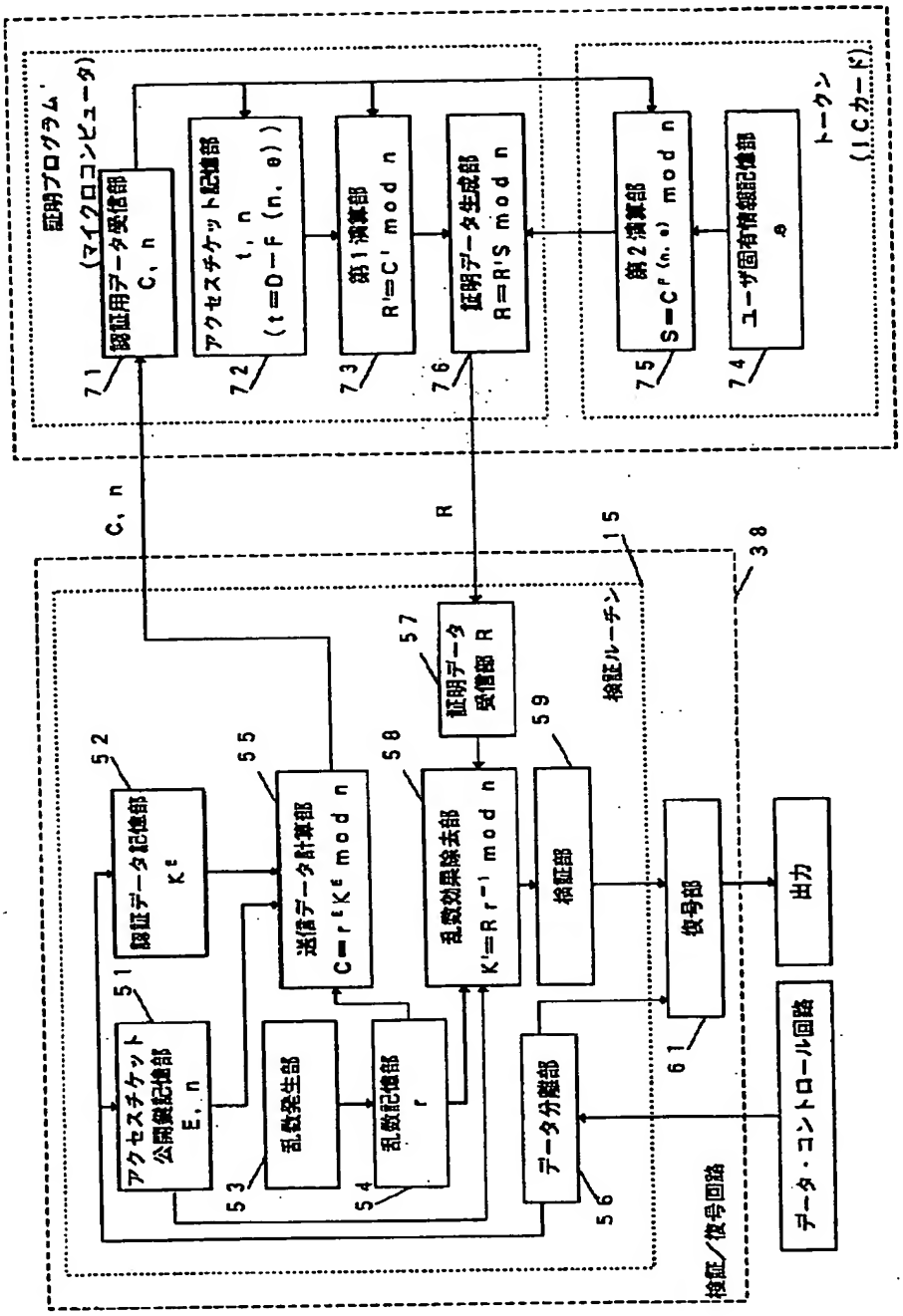


第４の実施例の構成図

【図１５】

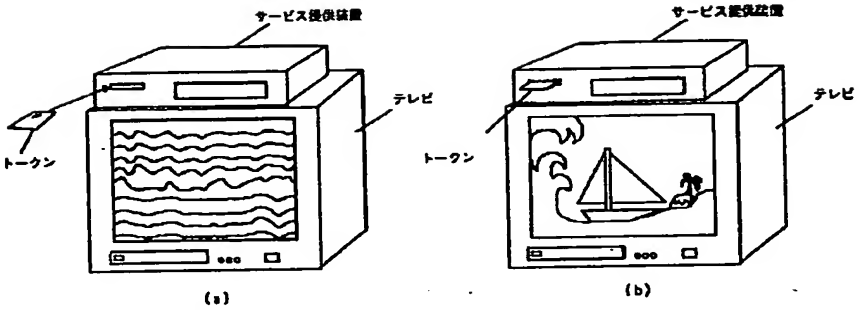

衛星信号
受信機
チューナ
誤り訂正回路／デスクランブル回路
データ・コントロール回路
検証／復号回路
デマルチプレクス回路
ビデオデコーダ
オーディオデコーダ
映像信号
オーディオ信号
デジタルデータ
バス
マイクロコンピュータ
RAM
EPROM
ユーザ・インタフェース回路
ICカード・インタフェース回路
モデム
リモコン／パネル
トークン（ICカード）
電話回線
第６の実施例の構成図

【図１６】

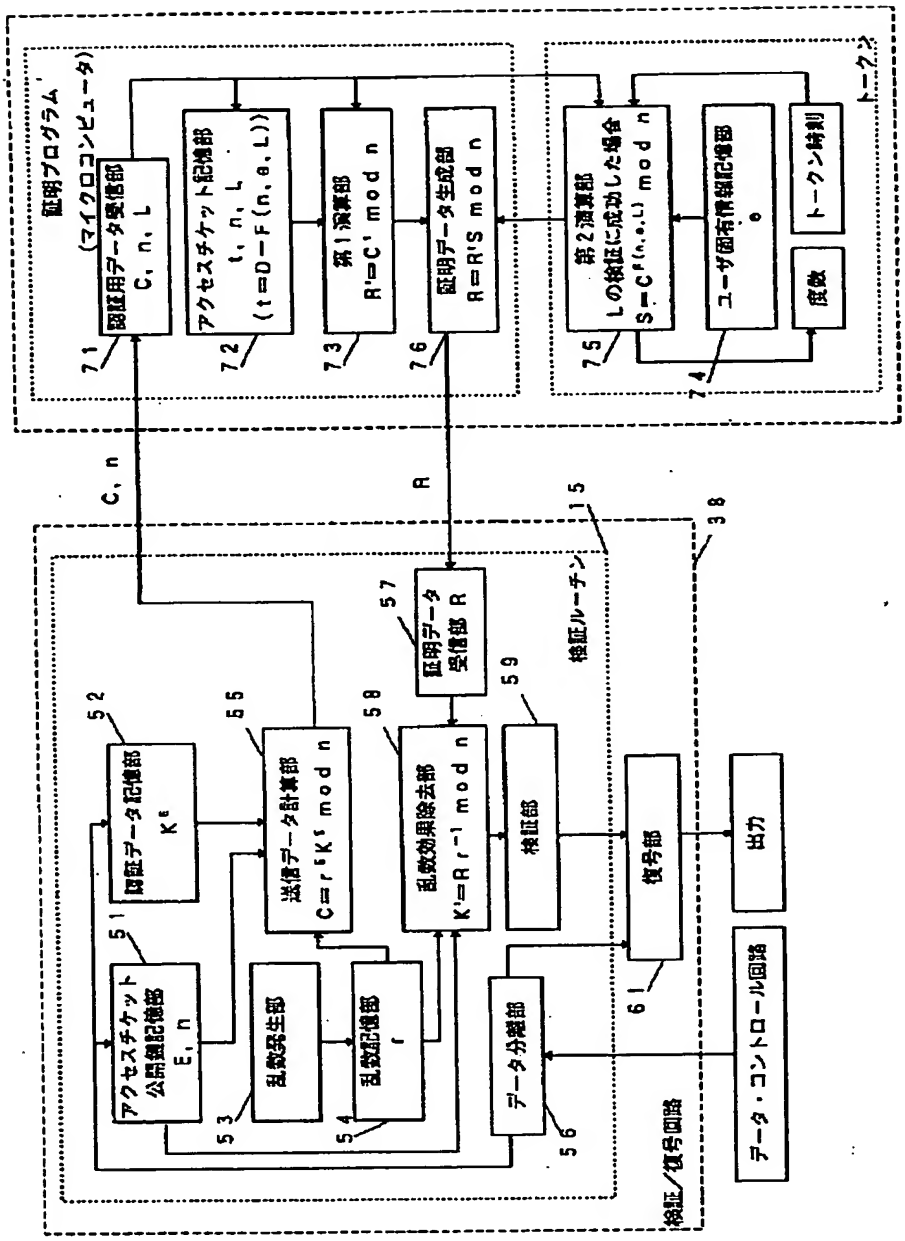


第６の実施例の構成図

【図１７】



【図１９】

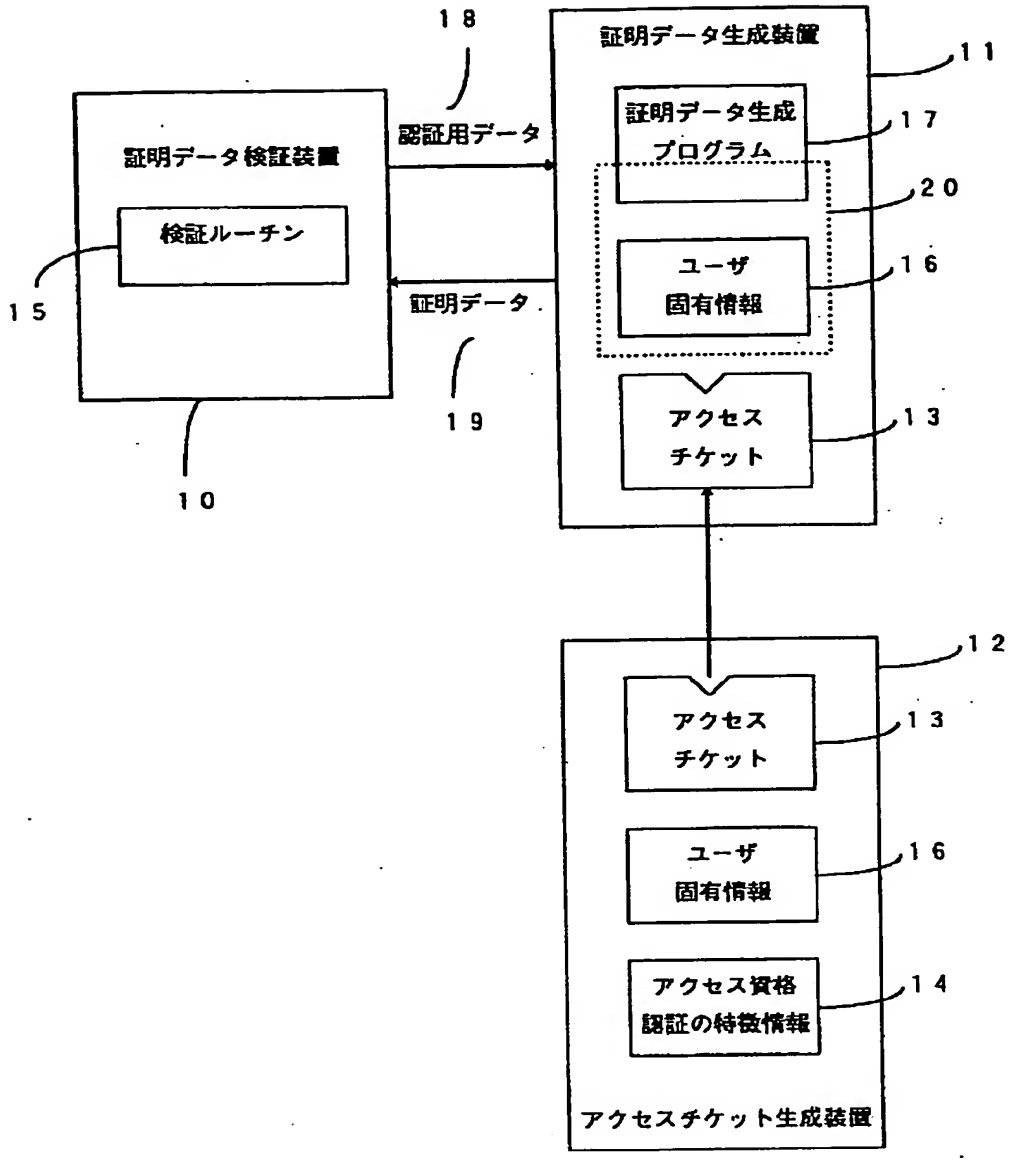


第６の実施例の構成図

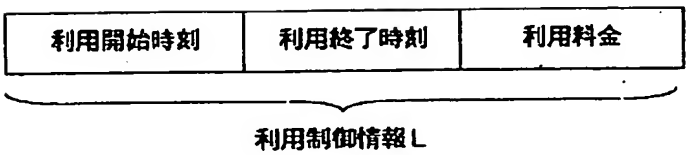
【手続補正書】
【提出日】平成９年１０月２９日
【手続補正１】
【補正対象書類名】図面

【補正対象項目名】全図
【補正方法】変更
【補正内容】

【図１】

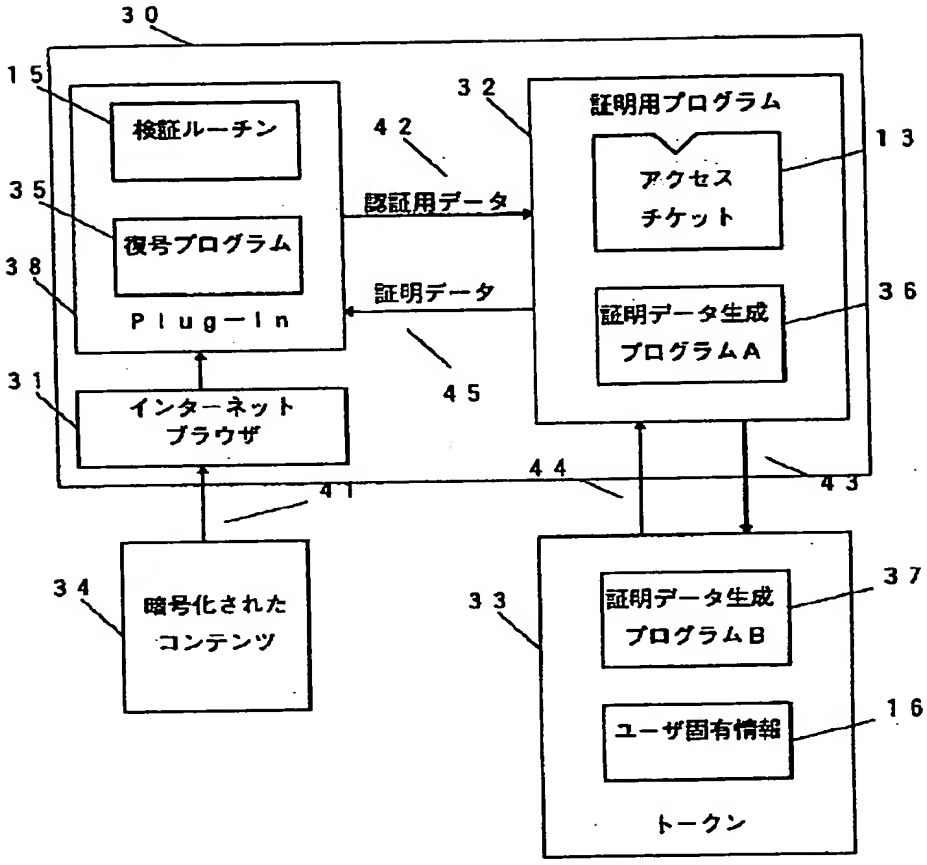


【図２０】

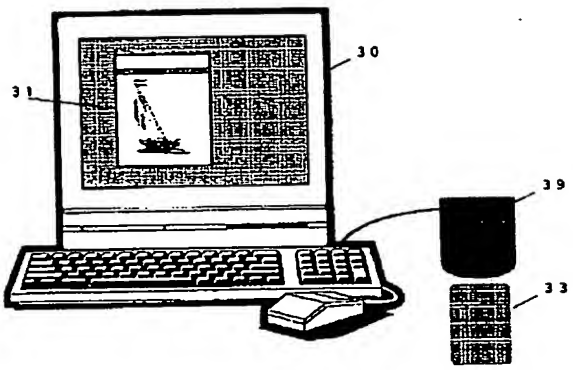


利用制御情報の構成図

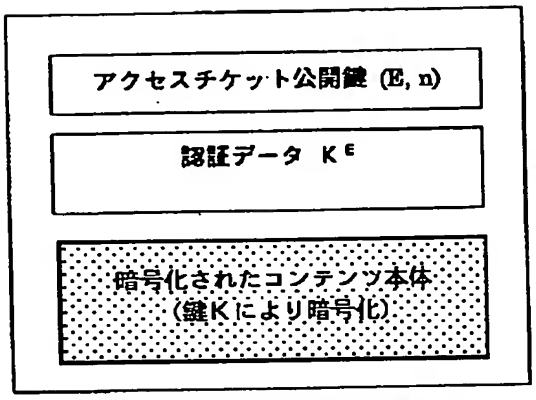
【図２】


３０
１５
検証ルーチン
３５
復号プログラム
３８
Ｐｌｕｇ－Ｉｎ
３１
インターネット
ブラウザ
３２
証明用プログラム
１３
アクセス
チケット
３６
証明データ生成
プログラムＡ
４２
認証用データ
証明データ
４５
４４
４３
４１
３４
暗号化された
コンテンツ
３３
３７
証明データ生成
プログラムＢ
１６
ユーザ固有情報
トークン

【図３】

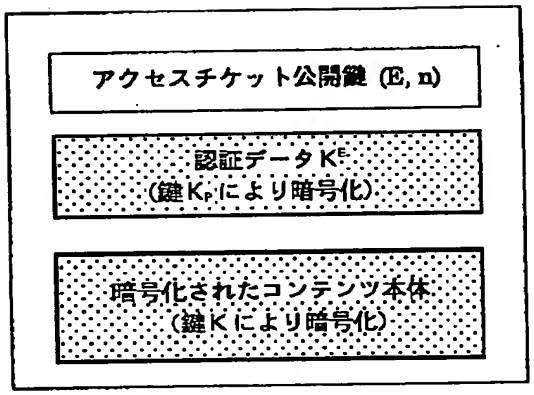


【図５】



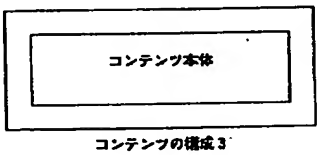
暗号化されたコンテンツの構成１

【図６】



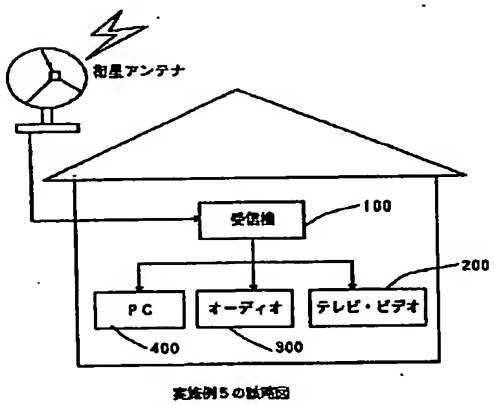
暗号化されたコンテンツの構成２

【図７】



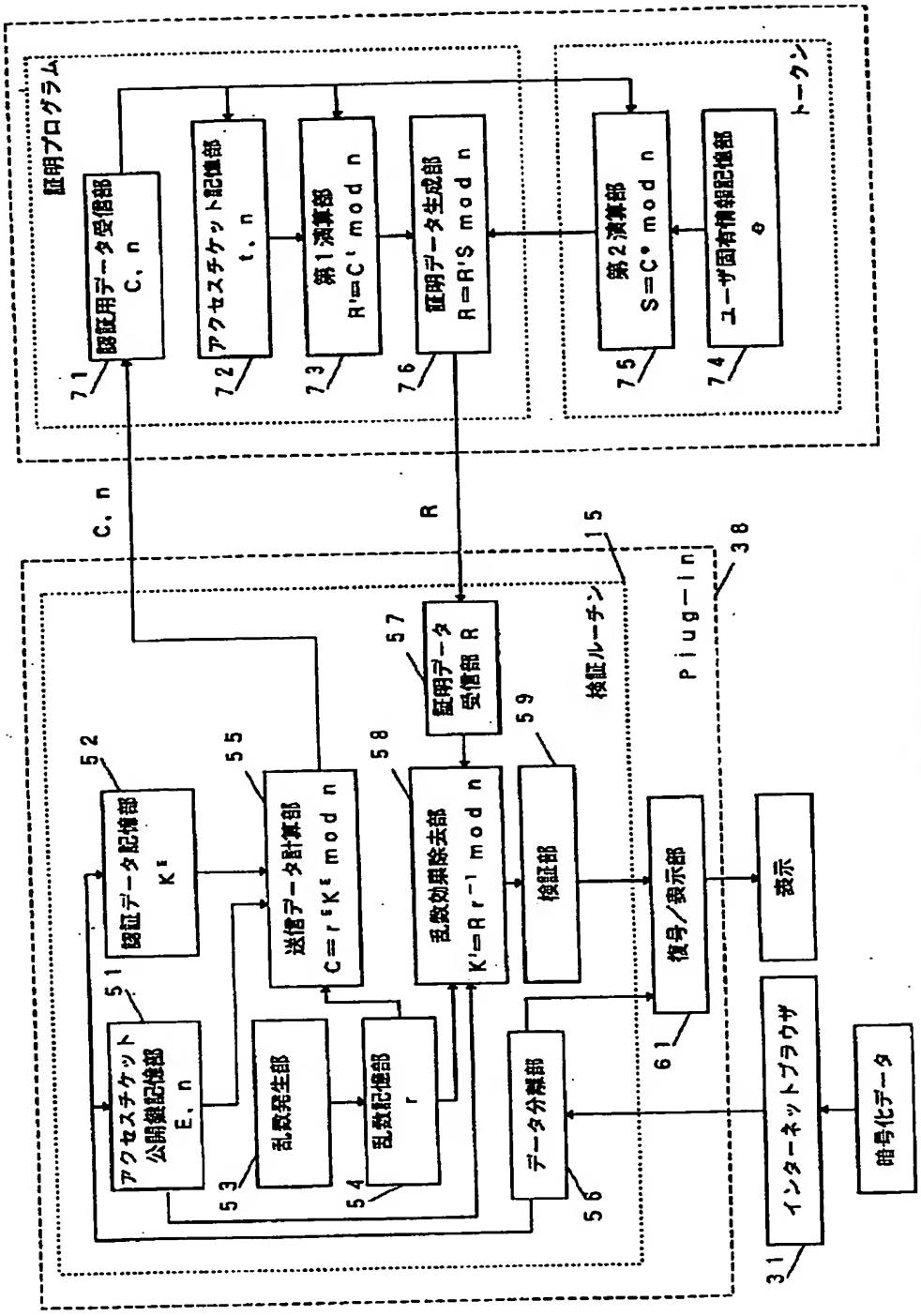
コンテンツの構成３

【図１５】



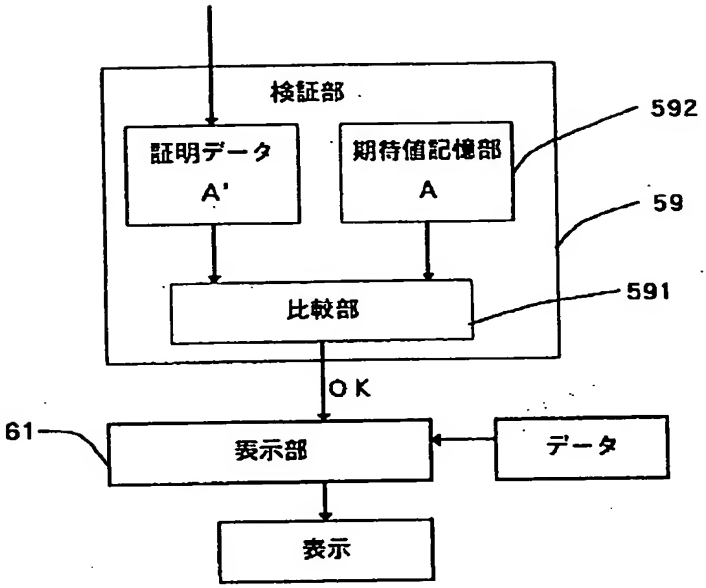
実施例５の説明図

【図４】



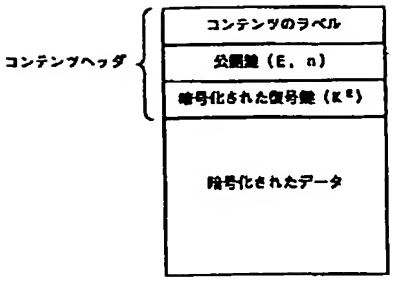
実施例１の詳細な構成例

【図８】



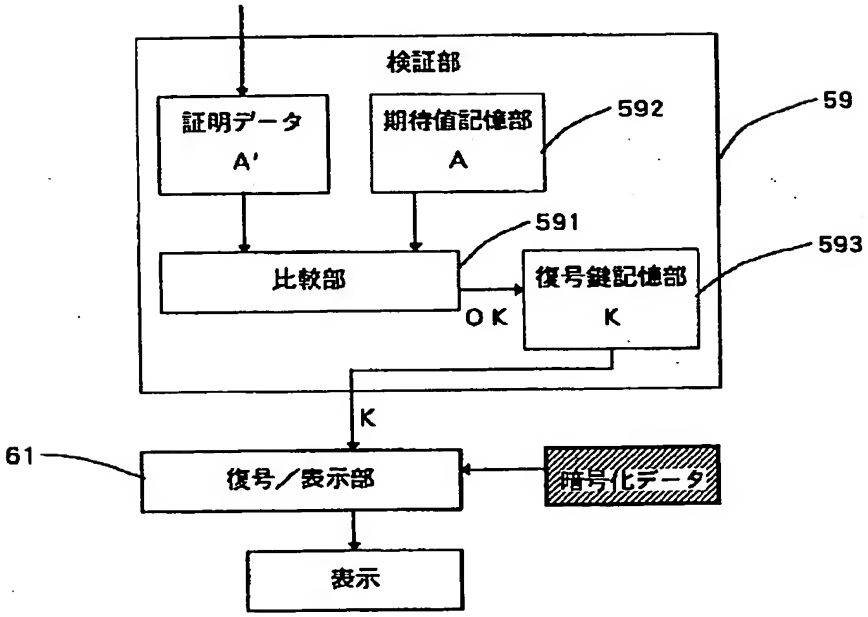
検証部の構成１

【図１６】



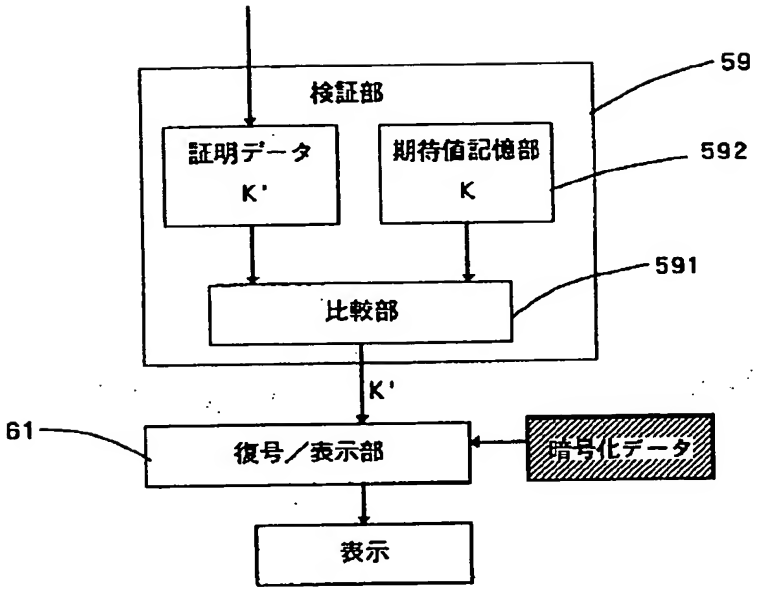
カプセル化されたコンテンツの構成図

【図９】



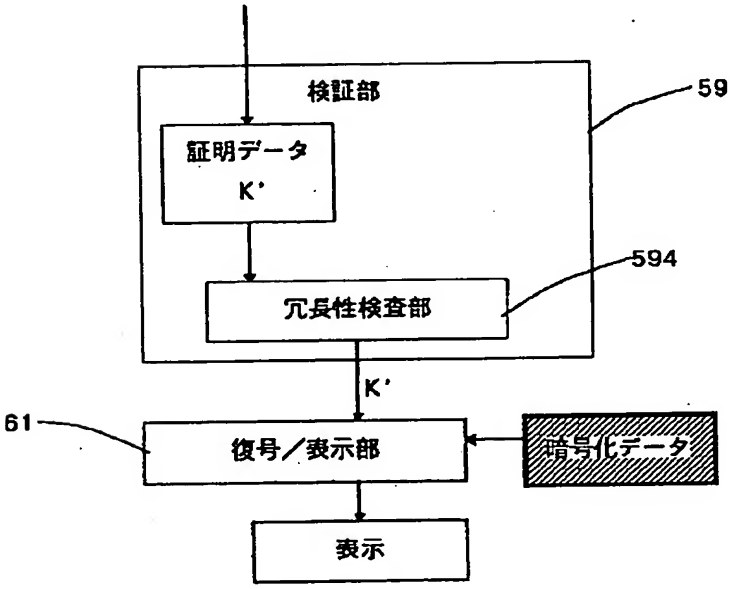
検証部の構成２

【図１０】



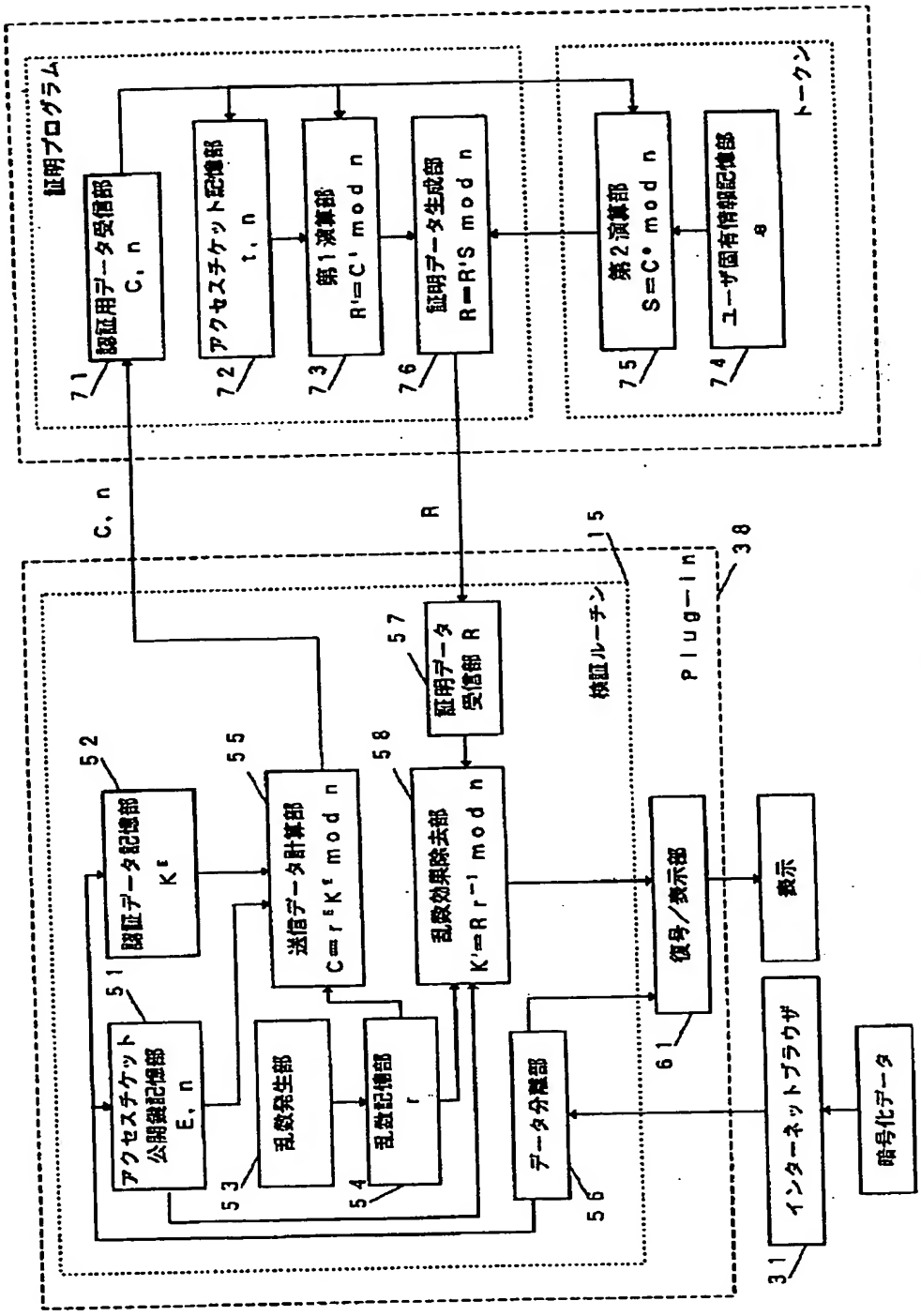
検証部の構成３

【図１１】



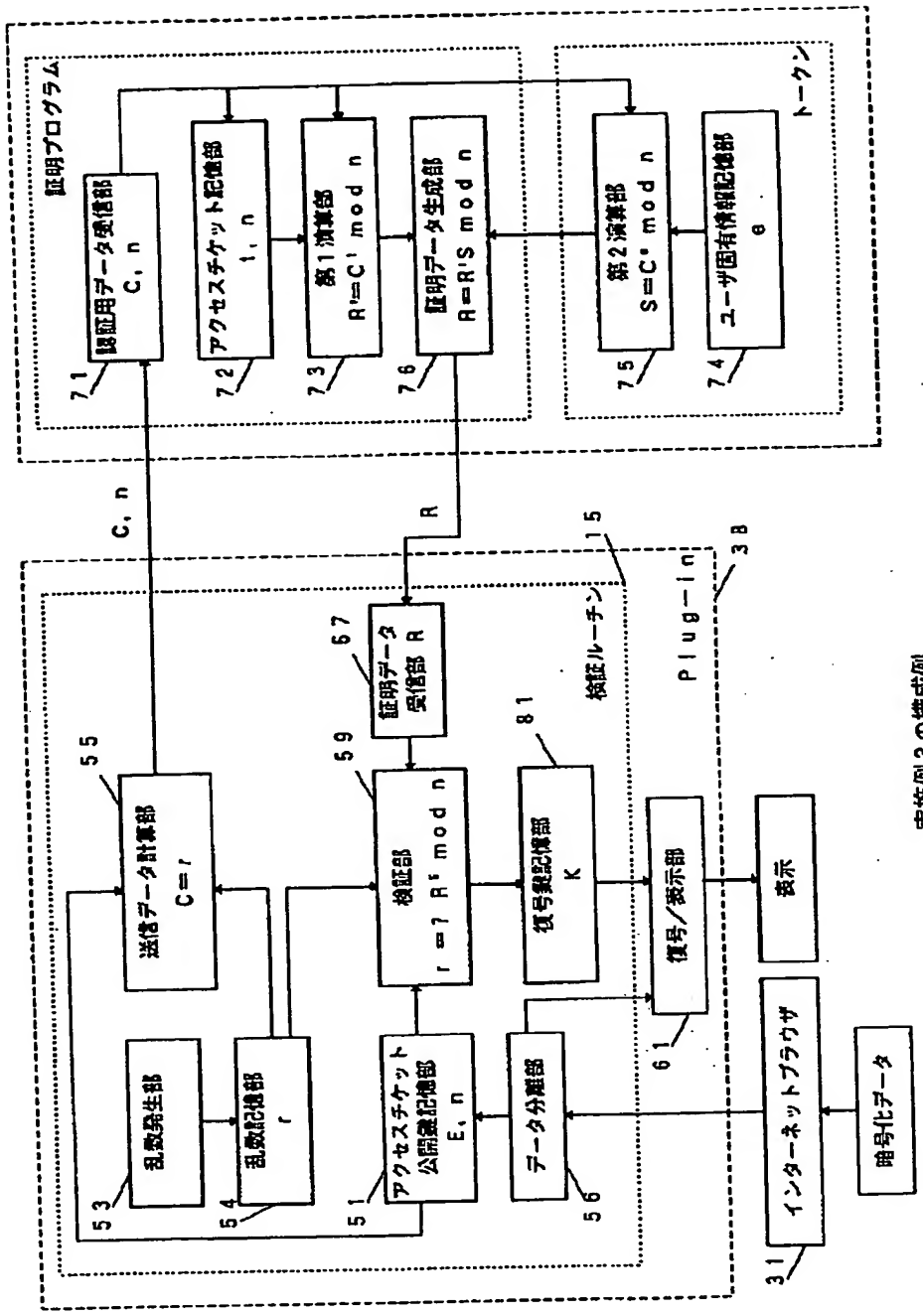
検証部の構成４

【図12】



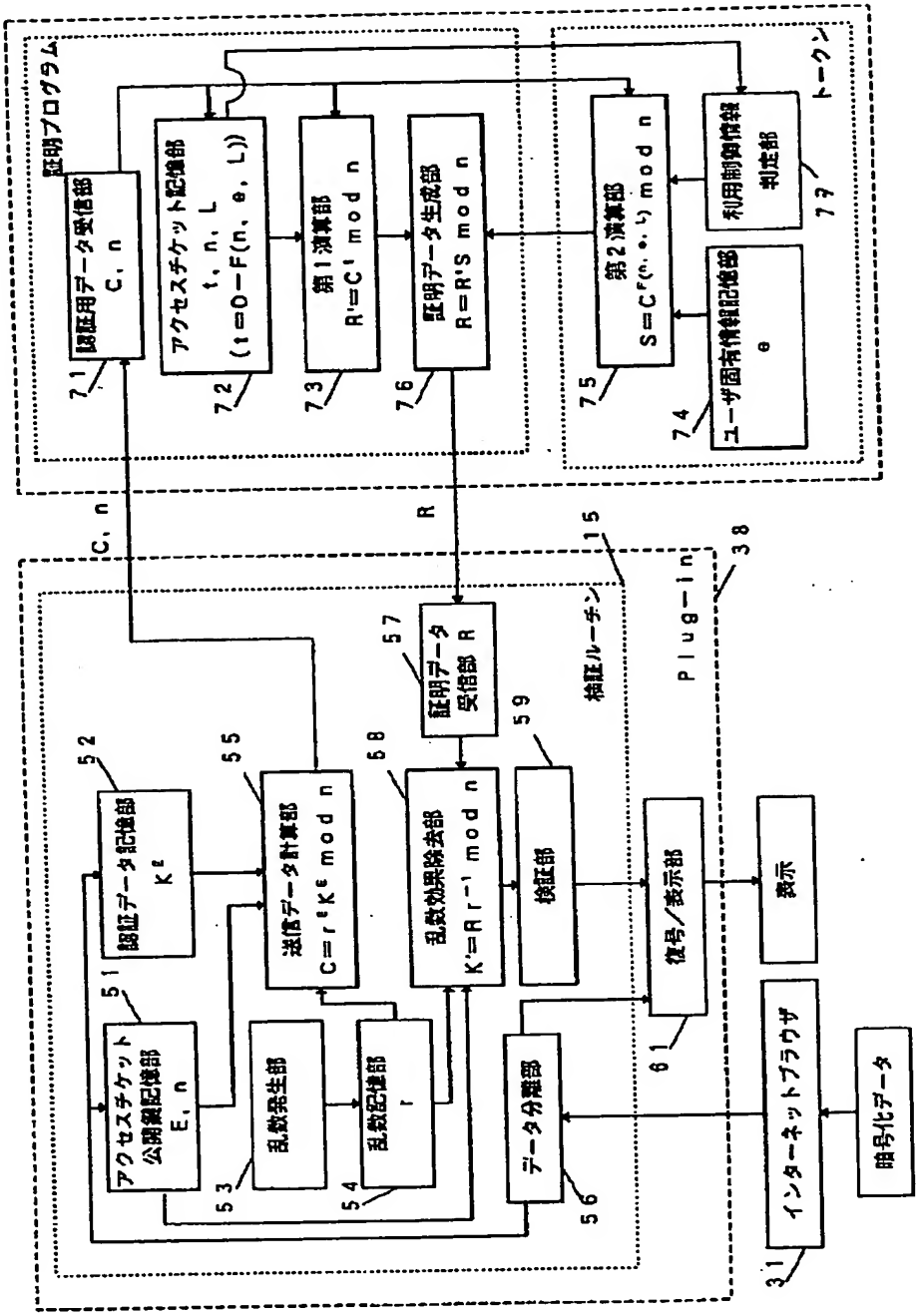
実施例2の構成例

【図１３】



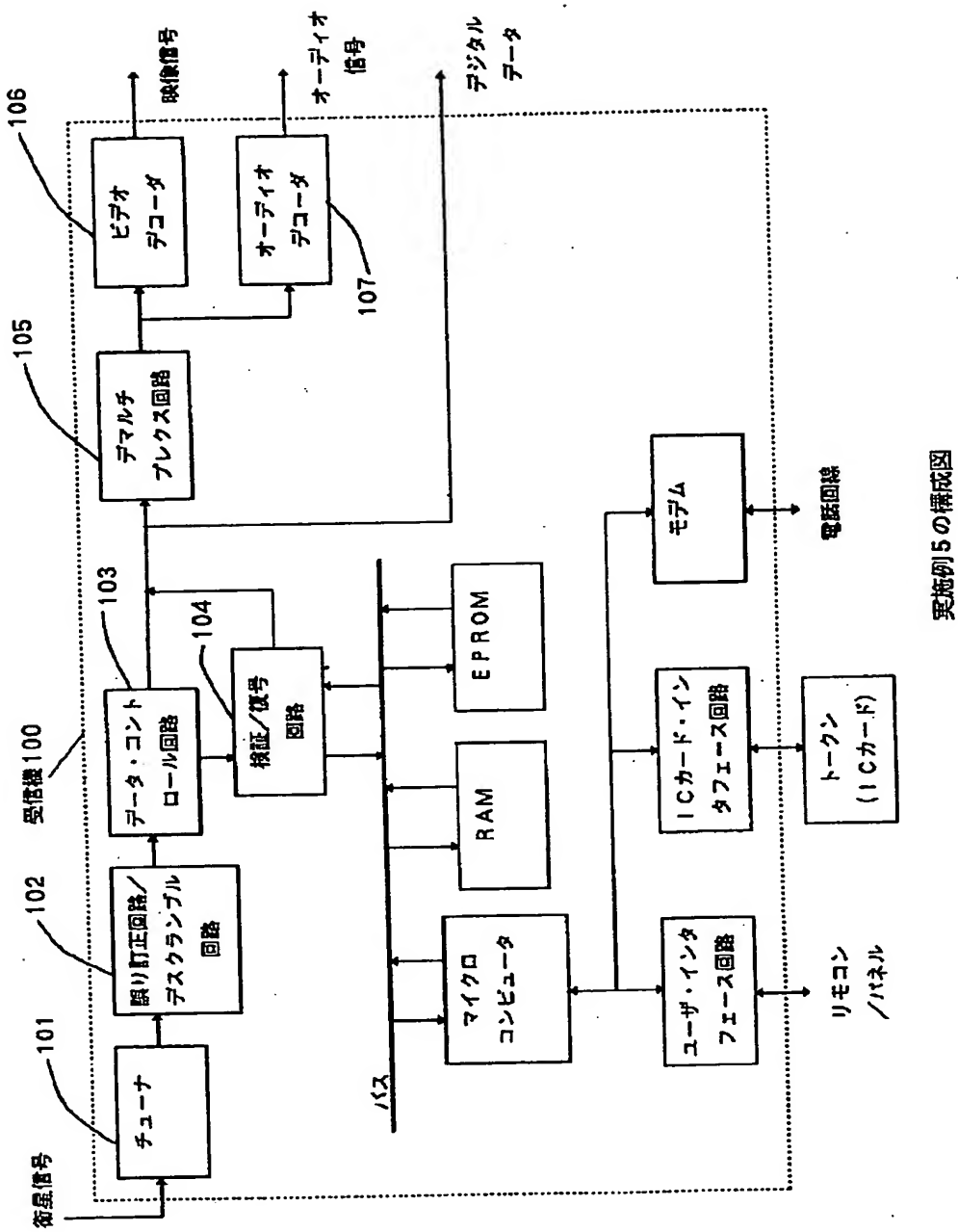
実施例３の構成例

【図１４】



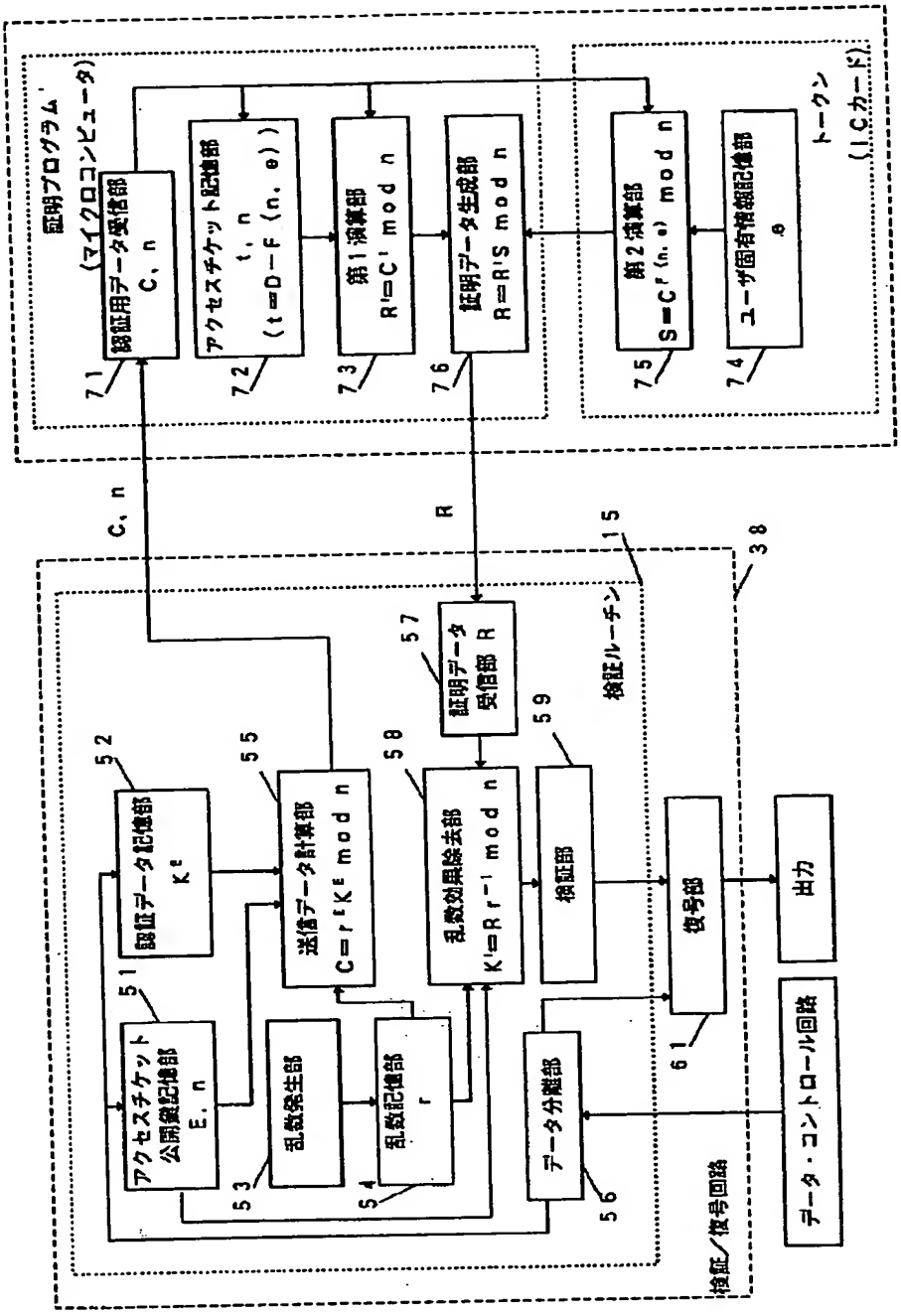
実施例４の構成図

【図１７】



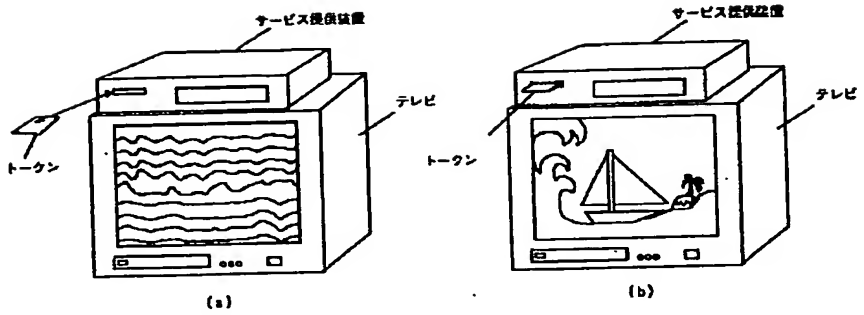
実施例５の構成図

【図１８】

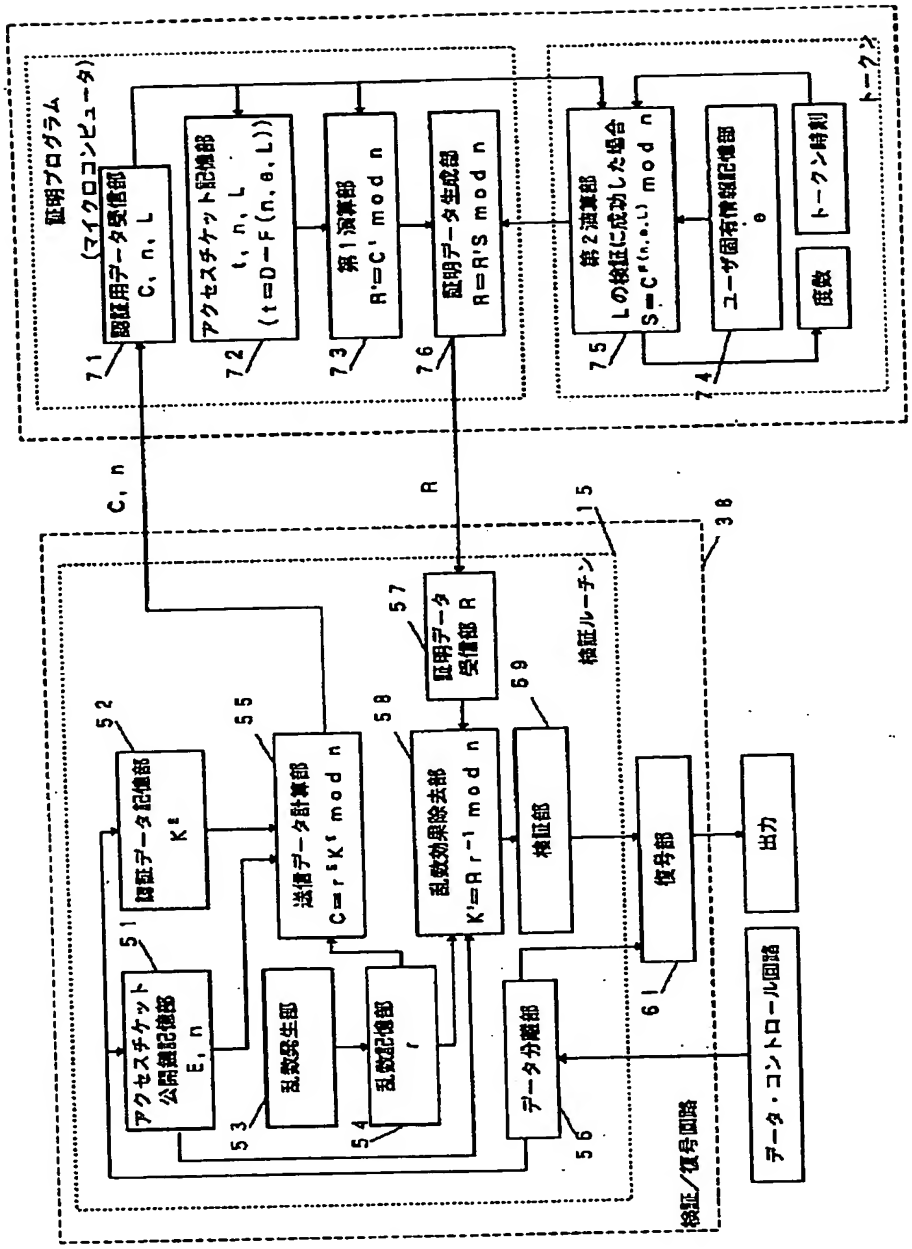


実施例５の構成図

【図１９】



【図21】



実施例16の構成図